DATE DUE

GAYLORD			PRINTED IN U.S.A.

Production Note

Cornell University Library produced this volume to replace the irreparably deteriorated original. It was scanned using Xerox software and equipment at 600 dots per inch resolution and compressed prior to storage using CCITT Group 4 compression. The digital data were used to create Cornell's replacement volume on paper that meets the ANSI Standard Z39.48-1984. The production of this volume was supported in part by the Commission on Preservation and Access and the Xerox Corporation. 1990.

Publications

OF THE

University of Pennsylvania

SERIES IN

MATHEMATICS

No. 3

GROUPS OF ORDER p^m WHICH CONTAIN CYCLIC SUBGROUPS OF ORDER p^{m-3}

BY

LEWIS IRVING NEIKIRK
SOMETIME HARRISON RESEARCH FELLOW IN MATHEMATICS

Published for the University
PHILADELPHIA
THE JOHN C. WINSTON CO., AGENTS
1006 ARCH STREET, PHILADELPHIA, PA.
1905

Publications

OF THE

University of Pennsylvania

SERIES IN

MATHEMATICS

No. 3

GROUPS OF ORDER p^m WHICH CONTAIN CYCLIC SUBGROUPS OF ORDER p^{m-3}

BY

LEWIS IRVING NEIKIRK

SOMETIME HARRISON RESEARCH FELLOW IN MATHEMATICS

Published for the University

PHILADELPHIA

THE JOHN C. WINSTON CO., AGENTS

1006 ARCH STREET, PHILADELPHIA, PA.

1905

INTRODUCTORY NOTE.

This monograph was begun in 1902–3. Class I, Class II, Part I, and the self-conjugate groups of Class III, which contain all the groups with independent generators, formed the thesis which I presented to the Faculty of Philosophy of the University of Pennsylvania in June, 1903, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

The entire paper was rewritten and the other groups added while the author was Research Fellow in Mathematics at the University.

I wish to express here my appreciation of the opportunity for scientific research afforded by the Fellowships on the George Leib Harrison Foundation at the University of Pennsylvania.

I also wish to express my gratitude to Professor George H. Hallett for his kind assistance and advice in the preparation of this paper, and especially to express my indebtedness to Professor Edwin S. Crawley for his support and encouragement, without which this paper would have been impossible.

LEWIS I. NEIKIRK.

UNIVERSITY OF PENNSYLVANIA,
May, 1905.

GROUPS OF ORDER p^m, WHICH CONTAIN CYCLIC SUBGROUPS OF ORDER p^{m-3}*

BY

LEWIS IRVING NEIKIRK

Introduction.

The groups of order p^m, which contain self-conjugate cyclic subgroups of orders p^{m-1}, and p^{m-2} respectively, have been determined by BURNSIDE,† and the number of groups of order p^m, which contain cyclic non-self-conjugate subgroups of order p^{m-2} has been given by MILLER.‡

Although in the present state of the theory, the actual tabulation of all groups of order p^m is impracticable, it is of importance to carry the tabulation as far as may be possible. In this paper *all groups of order* p^m (p being an odd prime) *which contain cyclic subgroups of order* p^{m-3} *and none of higher order* are determined. The method of treatment used is entirely abstract in character and, in virtue of its nature, it is possible in each case to give explicitly the generational equations of these groups. They are divided into three classes, and it will be shown that these classes correspond to the three partitions: $(m-3,\ 3)$, $(m-3,\ 2,\ 1)$ and $(m-3, 1, 1, 1)$, of m.

We denote by G an abstract group G of order p^m containing operators of order p^{m-3} and no operator of order greater than p^{m-3}. Let P denote one of these operators of G of order p^{m-3}. The p^3 power of every operator in G is contained in the cyclic subgroup $\{P\}$, otherwise G would be of order greater than p^m. The complete division into classes is effected by the following assumptions:

I. There is in G at least one operator Q_1, such that $Q_1^{p^2}$ is not contained in $\{P\}$.

II. The p^2 power of every operator in G is contained in $\{P\}$, and there is at least one operator Q_1, such that Q_1^p is not contained in $\{P\}$.

* Presented to the American Mathematical Society April 25, 1903.

† *Theory of Groups of a Finite Order*, pp. 75–81.

‡ Transactions, vol. 2 (1901), p. 259, and vol. 3 (1902), p. 383.

III. The pth power of every operator in G is contained in $\{P\}$.

The number of groups for Class I, Class II, and Class III, together with the total number, are given in the table below:

	I	II_1	II_2	II_3	II	III	Total
$p>3$, $m>8$	9	$20+p$	$6+2p$	$6+2p$	$32+5p$	23	$64+5p$
$p>3$, $m=8$	8	$20+p$	$6+2p$	$6+2p$	$32+5p$	23	$63+5p$
$p>3$, $m=7$	6	$20+p$	$6+2p$	$6+2p$	$32+5p$	23	$61+5p$
$p=3$, $m>8$	9	23	12	12	47	16	72
$p=3$, $m=8$	8	23	12	12	47	16	71
$p=3$, $m=7$	6	23	12	12	47	16	69

Class I.

1. *General notations and relations.*—The group G is generated by the two operators P and Q_1. For brevity we set *

$$Q_1^a P^b Q_1^c P^d \cdots = [a, b, c, d, \cdots].$$

Then the operators of G are given each uniquely in the form

$$[y, x] \qquad \binom{y=0,1,2,\cdots,p^3-1}{x=0,1,2,\cdots,p^{m-3}-1}.$$

We have the relation

(1) $$Q_1^{p^3} = P^{hp^3}.$$

There is in G, a subgroup H_1 of order p^{m-2}, which contains $\{P\}$ self-conjugately.† The subgroup H_1 is generated by P and some operator $Q_1^y P^x$ of G; it then contains Q_1^y and is therefore generated by P and $Q_1^{p^2}$; it is also self-conjugate in $H_2 = \{Q_1^p, P\}$ of order p^{m-1}, and H_2 is self-conjugate in G.

From these considerations we have the equations

(2)‡ $$Q_1^{-p^2} P Q_1^{p^2} = P^{1+kp^{m-4}},$$

* With J. W. Young, *On a certain group of isomorphisms*, American Journal of Mathematics, vol. 25 (1903), p. 206.

† Burnside: *Theory of Groups*, Art. 54, p. 64.

‡ *Ibid.*, Art. 56, p. 66.

(3) $$Q_1^{-p} P Q_1^p = Q_1^{\beta p^2} P^{\alpha_1},$$

(4) $$Q_1^{-1} P Q_1 = Q_1^{hp} P^{\alpha_1}.$$

2. *Determination of H_1. Derivation of a formula for* $[yp^2, x]^s$.— From (2), by repeated multiplication we obtain

$$[-p^2, x, p^2] = [0, x(1 + kp^{m-4})];$$

and by a continued use of this equation we have

$$[-yp^2, x, yp^2] = [0, x(1 + kp^{m-4})^y] = [0, x(1 + kyp^{m-4})] \quad (m > 4)$$

and from this last equation,

(5) $$[yp^2, x]^s = [syp^2, x\{s + k\tbinom{s}{2}yp^{m-4}\}].$$

3. *Determination of H_2. Derivation of a formula for* $[yp, x]^s$.— It follows from (3) and (5) that

$$[-p^2, 1, p^2] = \left[\beta\frac{\alpha_1^p - 1}{\alpha_1 - 1}p^2, \alpha_1^p\left\{1 + \frac{\beta k}{2}\frac{\alpha_1^p - 1}{\alpha_1 - 1}p^{m-4}\right\}\right] \quad (m > 4).$$

Hence, by (2),

$$\beta\frac{\alpha_1^p - 1}{\alpha_1 - 1}p^2 \equiv 0 \pmod{p^3},$$

$$\alpha_1^p\left\{1 + \frac{\beta k}{2}\frac{\alpha_1^p - 1}{\alpha_1 - 1}p^{m-4}\right\} + \beta\frac{\alpha_1^p - 1}{\alpha_1 - 1}hp^2 \equiv 1 + kp^{m-4} \pmod{p^{m-3}}.$$

From these congruences, we have for $m > 6$

$$\alpha_1^p \equiv 1 \pmod{p^3}, \qquad \alpha_1 \equiv 1 \pmod{p^2},$$

and obtain, by setting

$$\alpha_1 = 1 + \alpha_2 p^2,$$

the congruence

$$\frac{(1 + \alpha_2 p^2)^p - 1}{\alpha_2 p^3}(\alpha_2 + h\beta)p^3 \equiv kp^{m-4} \pmod{p^{m-3}};$$

and so

$$(\alpha_2 + h\beta)p^3 \equiv 0 \pmod{p^{m-4}},$$

since

$$\frac{(1 + \alpha_2 p^2)^p - 1}{\alpha_2 p^3} \equiv 1 \pmod{p^2}.$$

From the last congruences

(6) $$(\alpha_2 + h\beta)p^3 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

Equation (3) is now replaced by

(7) $$Q_1^{-p} P Q_1^{-p} = Q_1^{\beta p^2} P^{1+a_2p^2}.$$

From (7), (5), and (6)

$$[-yp, x, yp] = [\beta xyp^2, x\{1 + a_2yp^2\} + \beta k\tbinom{x}{2}yp^{m-4}].$$

A continued use of this equation gives

(8) $$\begin{aligned}[yp, x]^s = [\, & syp + \beta\tbinom{s}{2}xyp^2, \\ & xs + \tbinom{s}{2}\{a_2xyp^2 + \beta k\tbinom{x}{2}yp^{m-4}\} + \beta k\tbinom{s}{3}x^2yp^{m-4}].\end{aligned}$$

4. *Determination of G.*—From (4) and (8),

$$[-p, 1, p] = [Np, a_1^p + Mp^2].$$

From the above equation and (7),

$$a_1^p \equiv 1 \pmod{p^2}, \qquad a_1 \equiv 1 \pmod{p}.$$

Set $a_1 = 1 + a_2p$ and equation (4) becomes

(9) $$Q_1^{-1} P Q_1 = Q_1^{bp} P^{1+a_2p}.$$

From (9), (8) and (6)

$$[-p^2, 1, p^2] = \left[\frac{(1 + a_2p)^{p^2} - 1}{a_2p} bp, (1 + a_2p)^{p^2}\right],$$

and from (1) and (2)

$$\frac{(1 + a_2p)^{p^2} - 1}{a_2p} bp \equiv 0 \pmod{p^3},$$

$$(1 + a_2p)^{p^2} + bh\frac{(1 + a_2p)^{p^2} - 1}{a_2p}p \equiv 1 + kp^{m-4} \pmod{p^{m-3}}.$$

By a reduction similar to that used before,

(10) $$(a_2 + bh)p^3 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

The groups in this class are completely defined by (9), (1) and (10).

These defining relations may be presented in simpler form by a suitable choice of the second generator Q_1. From (9), (6), (8) and (10)

$$[1, x]^{p^3} = [p^3, xp^3] = [0, (x + h)p^3] \qquad (m > 6),$$

and, if x be so chosen that

$$x + h \equiv 0 \pmod{p^{m-6}},$$

$Q_1 P^x$ is an operator of order p^3 whose p^2 power is not contained in $\{P\}$. Let $Q_1 P^x = Q$. The group G is generated by Q and P, where

$$Q^{p^3} = 1, \qquad P^{p^{m-3}} = 1.$$

Placing $h = 0$ in (6) and (10) we find

$$\alpha_2 p^3 \equiv a_2 p^3 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

Let $\alpha_2 = \alpha p^{m-7}$, and $a_2 = ap^{m-7}$. Equations (7) and (9) are now replaced by

$$(11) \qquad \begin{aligned} Q^{-p} P Q^p &= Q^{\beta p^2} P^{1+\alpha p^{m-6}}, \\ Q^{-1} P Q &= Q^{bp} P^{1+ap^{m-6}}. \end{aligned}$$

As a direct result of the foregoing relations, the groups in this class correspond to the partition $(m-3, 3)$. From (11) we find

$$[-y, 1, y] = [byp, 1 + ayp^{m-6}] \qquad (m > 8).*$$

It is important to notice that by placing $y = p$ and p^2 in the preceding equation we find that

$$b \equiv \beta \pmod{p}, \ a \equiv \alpha \equiv k \pmod{p^3} (m > 7).\dagger$$

A combination of the last equation with (8) yields

$$(12) \qquad \begin{aligned} [-y, x, y] = [&bxyp + b^2\tbinom{x}{2} yp^2, \\ &x(1 + ayp^{m-6}) + ab\tbinom{x}{2} yp^{m-5} + ab^2\tbinom{x}{3} yp^{m-4}] \quad (m > 8).\ddagger \end{aligned}$$

From (12) we get

* For $m = 8$ it is necessary to add $a^2\binom{y}{2}p^4$ to the exponent of P and for $m = 7$ the terms $a(a + abp/2)\binom{y}{2}p^2 + a^3\binom{y}{3}p^3$ to the exponent of P, and the term $ab\binom{y}{2}p^2$ to the exponent of Q. The extra term $27ab^2k\binom{y}{3}$ is to be added to the exponent of P for $m = 7$ and $p = 3$.

† For $m = 7$, $ap^2 - a^2p^3/2 \equiv \alpha p^2 \pmod{p^4}$, $ap^3 \equiv kp^3 \pmod{p^4}$. For $m = 7$ and $p = 3$ the first of the above congruences has the extra terms $27(a^3 + ab\beta k)$ on the left side.

‡ For $m = 8$ it is necessary to add the term $a\binom{y}{2}xp^4$ to the exponent of P, and for $m = 7$ the terms $x\{a(a + abp/2)\binom{y}{2}p^2 + a^3\binom{y}{3}p^3\}$ to the exponent of P, with the extra term $27\,ab^2k\binom{y}{3}x$ for $p = 3$, and the term $ab\binom{y}{2}xp^2$ to the exponent of Q.

$$
\begin{aligned}
[y, x]^s = [ys + by\{(x + b\tbinom{x}{2}p)\tbinom{s}{2} + x\tbinom{s}{3}p\}p,& \\
(13) \qquad xs + ay\{(x + b\tbinom{x}{2}p + b^2\tbinom{x}{3}p^2)\tbinom{s}{2}& \\
+ (bx^2p + 2b^2x\tbinom{x}{2}p^2)\tbinom{s}{3} + bx^2\tbinom{s}{4}p^2\}p^{m-6}]& \qquad (m>8).^*
\end{aligned}
$$

5. *Transformation of the Groups.*—The general group G of Class I is specified, in accordance with the relations (2) (11) by two integers a, b which (see (11)) are to be taken mod p^3, mod p^2, respectively. Accordingly setting

$$a = a_1 p^\lambda,\ b = b_1 p^\mu,$$

where

$$dv[a_1, p] = 1,\ dv[b_1, p] = 1 \qquad (\lambda=0, 1, 2, 3;\ \mu=0, 1, 2),$$

we have for the group $G = G(a, b) = G(a, b)(P, Q)$ the generational determination:

$$G(a, b): \begin{cases} Q^{-1}PQ = Q^{b_1 p^{\mu+1}} P^{1+a_1 p^{m+\lambda-6}} \\ Q^{p^3} = 1,\ P^{p^{m-3}} = 1. \end{cases}$$

Not all of these groups however are distinct. Suppose that

$$G(a, b)(P, Q) \sim G(a', b')(P', Q'),$$

by the correspondence

$$C = \begin{bmatrix} Q, & P \\ Q_1', & P_1' \end{bmatrix},$$

where

$$Q_1' = Q'^{y'} P'^{x' p^{m-6}}, \qquad \text{and} \qquad P_1' = Q'^{y} P'^{x},$$

with y' and x prime to p.

Since

$$Q^{-1}PQ = Q^{bp}P^{1+ap^{m-6}},$$

then

$$Q_1'^{-1}P_1'Q_1' = Q_1'^{bp}P_1'^{1+ap^{m-6}},$$

---

* For $m=8$ it is necessary to add the term $\frac{1}{2}axy\binom{s}{2}[\frac{1}{3}y(2s-1)-1]p^4$ to the exponent of P, and for $m=7$ the terms

$$
\begin{aligned}
x\Big\{\frac{a}{2}\Big(a+\frac{ab}{2}p\Big)\Big(\frac{2s-1}{3}y-1\Big)\tbinom{s}{2}yp^2 + \frac{a^3}{3!}\Big(\tbinom{s}{2}y^2-(2s-1)y+2\Big)yp^3& \\
+\frac{a^2bxy^2}{2}\tbinom{s}{3}\frac{3s-1}{2}p^3+\frac{a^2b}{2}\Big(\frac{s(s-1)^2(s-4)}{4!}y-\tbinom{s}{3}\Big)yp^3\Big\}&,
\end{aligned}
$$

with the extra terms

$$27\,abxy\Big\{\frac{bk}{3!}[\tbinom{s}{2}y^2-(2s-1)y+2]\tbinom{s}{3}+x(b^2k+a^2)(2y^3+1)\tbinom{s}{3}\Big\}$$

for $p=3$, to the exponent of P, and the terms

$$\frac{ab}{2}\Big\{2s-\tfrac{1}{3}y-1\Big\}\tbinom{s}{2}xyp^2$$

to the exponent of Q.

or in terms of Q', and P'

$$[y + b'xy'p + b'^2\binom{x}{2}y'p^2,\ x(1 + a'y'p^{m-6}) + a'b'\binom{x}{2}y'p^{m-5} + a'b'^2\binom{x}{3}y'p^{m-4}] = [y + by'p,\ x + (ax + bx'p)p^{m-6}] \qquad (m > 8)$$

and

(14) $$by' \equiv b'xy' + b'^2\binom{x}{2}y'p \pmod{p^2},$$

(15) $$ax + bx'p \equiv a'y'x + a'b'\binom{x}{2}y'p + a'b'^2\binom{x}{3}y'p^2 \pmod{p^3}.$$

The necessary and sufficient condition for the simple isomorphism of these two groups $G(a, b)$ and $G(a', b')$ is, that the above congruences shall be consistent and admit of solution for x, y, x' and y'. The congruences may be written

$$b_1 p^{\mu} \equiv b_1' x p^{\mu'} + b_1'^2\binom{x}{2}p^{2\mu'+1} \pmod{p^2},$$

$$a_1 x p^{\lambda} + b_1 x' p^{\mu+1} \equiv y'\{a_1' x p^{\lambda'} + a_1' b_1'\binom{x}{2}p^{\lambda'+\mu'+1} + a_1' b_1'^2\binom{x}{3}p^{\lambda'+2\mu'+2}\} \pmod{p^3}.$$

Since $dv[x, p] = 1$ the first congruence gives $\mu = \mu'$ and x may always be so chosen that $b_1 = 1$.

We may choose y' in the second congruence so that $\lambda = \lambda'$ and $a_1 = 1$ except for the cases $\lambda' \geqq \mu + 1 = \mu' + 1$ when we will so choose x' that $\lambda = 3$.

The type groups of Class I for $m > 8$ * are then given by

(I) $$G(p^{\lambda}, p^{\mu}) : Q^{-1}PQ = Q^{p^{1+\mu}}P^{1+p^{m-6+\lambda}},\quad Q^{p^3} = 1,\quad P^{p^{m-3}} = 1$$

$$\begin{pmatrix}\mu = 0, 1, 2;\ \lambda = 0, 1, 2;\ \lambda \geqq \mu; \\ \mu = 0, 1, 2;\ \lambda = 3\end{pmatrix}.$$

Of the above groups $G(p^{\lambda}, p^{\mu})$ the groups for $\mu = 2$ have the cyclic subgroup $\{P\}$ self-conjugate, while the group $G(p^3, p^2)$ is the abelian group of type $(m - 3, 3)$.

Class II.

1. *General relations.*

There is in G an operator Q_1 such that $Q_1^{p^2}$ is contained in $\{P\}$ while Q_1^p is not.

(1) $$Q_1^{p^2} = P^{hp^2}.$$

---

* For $m = 8$ the additional term ayp appears on the left side of the congruence (14) and $G(1, p^2)$ and $G(1, p)$ become simply isomorphic. The extra terms appearing in congruence (15) do not effect the result. For $m = 7$ the additional term ay appears on the left side of (14) and $G(1, 1)$, $G(1, p)$, and $G(1, p^2)$ become simply isomorphio, also $G(p, p)$ and $G(p, p^2)$.

The operators Q_1 and P either generate a subgroup H_2 of order p^{m-1}, or the entire group G.

Section 1.

2. *Groups with independent generators.*

Consider the first possibility in the above paragraph. There is in H_2, a subgroup H_1 of order p^{m-2}, which contains $\{P\}$ self-conjugately.* H_1 is generated by Q_1^p and P. H_2 contains H_1 self-conjugately and is itself self-conjugate in G.

From these considerations

(2) $$Q_1^{-p} P Q_1^p = P^{1+kp^{m-4}}, \dagger$$

(3) $$Q_1^{-1} P Q = Q_1^{\beta p} P^{a_1}.$$

3. *Determination of H_1 and H_2.*

From (2) we obtain

(4) $$[yp, x]^s = [syp, x\{s + k\tbinom{s}{2} yp^{m-4}\}] \qquad (m>4),$$

and from (3) and (4)

$$[-p, 1, p] = \left[\frac{\alpha_1^p - 1}{\alpha_1 - 1}\beta p,\ \alpha_1^p\left\{1 + \frac{\beta k}{2}\frac{\alpha_1^p - 1}{\alpha_1 - 1}p^{m-4}\right\}\right].$$

A comparison of the above equation with (2) shows that

$$\frac{\alpha_1^p - 1}{\alpha_1 - 1}\beta p \equiv 0 \pmod{p^2},$$

$$\alpha_1^p\left\{1 + \frac{\beta k}{2}\frac{\alpha_1^p - 1}{\alpha_1 - 1}p^{m-4}\right\} + \frac{\alpha_1^p - 1}{\alpha_1 - 1}\beta h p \equiv 1 + kp^{m-4} \pmod{p^{m-3}},$$

and in turn

$$\alpha_1^p \equiv 1 \pmod{p^2}, \qquad \alpha_1 \equiv 1 \pmod{p} \qquad (m>5).$$

Placing $\alpha_1 = 1 + \alpha_2 p$ in the second congruence, we obtain as in Class I

(5) $$(\alpha_2 + \beta h)p^2 \equiv kp^{m-4} \pmod{p^{m-3}} \qquad (m>5).$$

Equation (3) now becomes

(6) $$Q_1^{-1} P Q_1 = Q^{\beta} P^{1+\alpha_2 p}.$$

The generational equations of H_2 will be simplified by using an operator of order p^2 in place of Q_1.

---

* BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

† *Ibid.*, Art. 56, p. 66.

From (5), (6) and (4)

$$[y, x]^s = [sy + U_s p, sx + W_s p]$$

in which

$$U_s = \beta \tbinom{s}{2} xy,$$

$$W_s = \alpha_2 \tbinom{s}{2} xy + \{ \beta k [\tbinom{s}{2}\tbinom{x}{2} + \tbinom{s}{3} x^2 y] + \tfrac{1}{2}\alpha k [\tfrac{1}{3!} s(s-1)(2s-1)y^2 - \tbinom{s}{2} y] x \} p^{m-5}.$$

Placing $s = p^2$ and $y = 1$ in the above

$$[Q_1 P^x]^{p^2} = Q_1^{p^2} P^{xp^2} = P^{(x+h)p^2}.$$

If x be so chosen that

$$(x + h) \equiv 0 \pmod{p^{m-5}} \qquad (m > 5)$$

$Q_1 P^x$ will be the required Q of order p^2.

Placing $h = 0$ in congruence (5) we find

$$\alpha_2 p^2 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

Let $\alpha_2 = \alpha p^{m-6}$. H_2 is then generated by

$$Q^{p^2} = 1, \qquad P^{p^{m-3}} = 1.$$

(7) $$Q^{-1} P Q = Q^{\beta p} P^{1+\alpha p^{m-5}}.$$

Two of the preceding formulæ now become

(8) $$[-y, x, y] = [\beta xyp, x(1 + \alpha y p^{m-5}) + \beta k \tbinom{x}{2} y p^{m-4}],$$

(9) $$[y, x]^s = [sy + U_s p, xs + W_s p^{m-5}],$$

where

$$U_s = \beta \tbinom{s}{2} xy$$

and

$$W_s = \alpha \tbinom{s}{2} xy + \beta k \{ \tbinom{s}{2}\tbinom{x}{2} + \tbinom{s}{3} x^2 \} yp \qquad (m > 6).*$$

4. *Determination of G.*

Let R_1 be an operation of G not in H_2. R_1^p is in H_2. Let

(10) $$R_1^p = Q^{\lambda p} P^{\mu p}.$$

Denoting $R_1^a Q^b P^c R_1^d Q^e P^f \cdots$ by the symbol $[a, b, c, d, e, f, \cdots]$, all the operations of G are contained in the set $[z, y, x]$; $z = 0, 1, 2, \cdots, p-1$; $y = 0, 1, 2, \cdots, p^2 - 1$; $x = 0, 1, 2, \cdots, p^{m-3} - 1$.

---

* For $m = 6$ it is necessary to add the terms

$$\frac{\alpha k}{2} \left\{ \frac{s(s-1)(2s-1)}{3!} y^2 - \tbinom{s}{2} y \right\} p \text{ to } W_s.$$

The subgroup H_2 is self-conjugate in G. From this

$$(11) \qquad R_1^{-1} P R_1 = Q^{b_1} P^{a_1},$$

$$(12) \qquad R_1^{-1} Q R_1 = Q^{d_1} P^{c_1 p^{m-6}}.*$$

In order to ascertain the forms of the constants in (11) and (12) we obtain from (12), (11), and (9)

$$[-p, 1, 0, p] = [0, d_1^p + Mp, Np^{m-5}].$$

By (10) and (8)

$$R_1^p Q R_1^p = P^{-\mu p} Q P^{\mu p} = Q P^{-\alpha\mu p^{m-4}}.$$

From these equations we obtain

$$d_1^p \equiv 1 \pmod{p} \quad \text{and} \quad d_1 \equiv 1 \pmod{p}.$$

Let $d_1 = 1 + dp$. Equation (12) is replaced by

$$(13) \qquad R_1^{-1} Q R_1 = Q^{1+dp} P^{c_1 p^{m-6}}.$$

From (11), (13) and (9)

$$[-p, 0, 1, p] = \left[\frac{a_1^p - 1}{a_1 - 1} b_1 + Kp,\ a_1^p + b_1 L p^{m-5}\right]$$

in which

$$K = a_1 b_1 \beta \sum_1^{p-1} \binom{a_1^y}{2}.$$

By (10) and (8)

$$R_1^{-p} P R_1^p = Q^{-\lambda p} P Q^{\lambda p} = P^{1+\alpha\lambda p^{m-4}},$$

and from the last two equations

$$a_1^p \equiv 1 \pmod{p^{m-5}}$$

and

$$a_1 \equiv 1 \pmod{p^{m-6}}\ (m > 6); \qquad a_1 \equiv 1 \pmod{p}\ (m = 6).$$

Placing $a_1 = 1 + a_2 p^{m-6}$ $(m > 6)$; $a_1 = 1 + a_2 p$ $(m = 6)$.

$$K \equiv 0 \pmod{p}, \dagger$$

and

$$\frac{a_1^p - 1}{a_1 - 1} b_1 \equiv b_1 p \equiv 0 \pmod{p^2},\ b_1 \equiv 0 \pmod{p}.$$

Let $b_1 = bp$ and we find

$$a_1^p \equiv 1 \pmod{p^{m-4}}, \qquad a_1 \equiv 1 \pmod{p^{m-5}}.$$

---

* BURNSIDE, *Theory of Groups*, Art. 24, p. 27.

† K has an extra term for $m = 6$ and $p = 3$, which reduces to $3b_1c_1$. This does not affect the reasoning except for $c_1 = 2$. In this case change P^2 to P and c_1 becomes 1.

Let $a_1 = 1 + a_3 p^{m-5}$ and equation (11) is replaced by

(14) $$R_1^{-1} P R_1 = Q^{bp} P^{1+a_3 p^{m-5}}.$$

The preceding relations will be simplified by taking for R_1 an operator of order p. This will be effected by two transformations.

From (14), (9) and (13)

$$[1, y]^p = \left[p, yp, \frac{-c_1 y}{2} p^{m-4}\right] = \left[0, (\lambda + y)p, \mu p - \frac{c_1 y}{2} p^{m-4}\right],^*$$

and if y be so chosen that

$$\lambda + y \equiv 0 \pmod{p},$$

$R_2 = R_1 Q^y$ is an operator such that R_2^p is in $\{P\}$.

Let

$$R_2^p = P^{lp}.$$

Using R_2 in the place of R_1, from (15), (9) and (14)

$$[1, 0, x]^p = \left[p, 0, xp + \frac{ax}{2} p^{m-4}\right] = \left[0, 0, (x + l)p + \frac{ax}{2} p^{m-4}\right],$$

and if x be so chosen that

$$x + l + \frac{ax}{2} p^{m-5} \equiv 0 \pmod{p^{m-4}},$$

then $R = R_2 P^x$ is the required operator of order p.

$R^p = 1$ is permutable with both Q and P. Preceding equations now assume the final forms

(15) $$Q^{-1} P Q = Q^{\beta p} P^{1+\alpha p^{m-5}},$$

(16) $$R^{-1} P R = Q^{bp} P^{1+ap^{m-4}},$$

(17) $$R^{-1} Q R = Q^{1+dp} P^{cp^{m-4}},$$

with $R^p = 1$, $Q^{p^2} = 1$, $P^{p^{m-3}} = 1$.

The following derived equations are necessary

(18) $[0, -y, x, 0, y] = [0, \beta xyp, x(1 + \alpha y p^{m-5}) + \alpha\beta\binom{x}{2} y p^{m-4}],\dagger$

(19) $[-y, 0, x, -y] = [0, bxyp, x(1 + ayp^{m-4}) + ab\binom{x}{2} y p^{m-4}]$,

(20) $[-y, x, 0, y] = [0, x(1 + dyp), cxyp^{m-4}]$.

---

* The extra terms appearing in the exponent of P for $m = 6$ do not alter the result.

† For $m = 6$ the term $a^2\binom{x}{2} xp^2$ must be added to the exponent of P in (18).

From a consideration of (18), (19) and (20) we arrive at the expression for a power of a general operator of G.

$$(21) \qquad [z, y, x]^s = [sz, sy + U_s p, sx + V_s p^{m-5}],$$

where

$$U_s = \binom{s}{2}\{bxz + \beta xy + dyz\},$$

$$V_s = \binom{s}{2}\{axy + [axz + a\beta\binom{x}{2}y + cyz + ab\binom{x}{2}z]p\}$$
$$+ a\binom{s}{3}\{bxz + \beta xy + dyz\}xp.*$$

5. *Transformation of the groups.* All groups of this section are given by equations (15), (16), and (17) with $a, b, \beta, c, d = 0, 1, 2, \cdots, p-1$, and $\alpha = 0, 1, 2, \cdots, p^2 - 1$, independently. Not all these groups, however, are distinct. Suppose that G and G' of the above set are simply isomorphic and that the correspondence is given by

$$C = \begin{bmatrix} R, & Q, & P \\ R_1', & Q_1', & P_1' \end{bmatrix},$$

in which

$$R_1' = R'^{z''} Q'^{y''p} P'^{x''p^{m-4}},$$

$$Q_1' = R'^{z'} Q'^{y'} P'^{x'p^{m-5}},$$

$$P_1' = R'^{z} Q'^{y} P'^{x},$$

where x, y' and z'' *are prime* to p.

The operators R_1', Q_1', and P_1' must be independent since R, Q, and P are, and that this is true is easily verified. The lowest power of Q_1' in $\{P_1'\}$ is $Q_1'^{p^2} = 1$ and the lowest power of R_1' in $\{Q_1', P_1'\}$ is $R_1'^p = 1$. Let $Q_1'^{s'} = P_1'^{sp^{m-5}}$.

This in terms of R', Q', and P' is

$[s'z', y'\{s' + d'\binom{s'}{2}z'p\}, s'x'p^{m-5} + c'\binom{s'}{2}y'z'p^{m-4}] = [0, 0, sxp^{m-5}]$.

From this equation s' is determined by

$$s'z' \equiv 0 \pmod{p}$$

$$y'\{s' + d'\binom{s}{2}z'p\} \equiv 0 \pmod{p^2},$$

which give

$$s'y' \equiv 0 \pmod{p^2}.$$

* When $m = 6$ the following terms are to be added to V_s:

$$\frac{a^2x}{2}\left\{\frac{s(s-1)(2s-1)}{3!}y^2 - \binom{s}{2}y\right\}p.$$

Since y' is prime to p

$$s' \equiv 0 \ (\mathrm{mod}\ p^2)$$

and the lowest power of Q_1' contained in $\{P_1'\}$ is $Q_1'^{p^2} = 1$.

Denoting by $R_1'^{s''}$ the lowest power of R_1' contained in $\{Q_1', P_1'\}$.

$$R_1'^{s''} = Q_1'^{s'p} P_1'^{sp^{m-4}}.$$

This becomes in terms of R', Q', and P'

$$[s''z'', s''y''p, s''x''p^{m-4}] = [0, s'y'p, \{s'x' + sx\}p^{m-4}].$$

s'' is now determined by

$$s''z'' \equiv 0 \ (\mathrm{mod}\ p)$$

and since z'' is prime to p

$$s'' \equiv 0 \ (\mathrm{mod}\ p).$$

The lowest power of R_1' contained in $\{Q_1', P'\}$ is therefore $R_1'^p = 1$.

Since R, Q, and P satisfy equations (15), (16), and (17) R_1', Q_1', and P_1' also satisfy them. Substituting in these equations the values of R_1', Q_1', and P_1' and reducing we have in terms of R', Q', and P'

(22) $[z, y + \theta_1 p, x + \phi_1 p^{m-5}] = [z, y + \beta y'p, x(1 + ap^{m-5}) + \beta xp^{m-4}]$,

(23) $[z, y + \theta_2 p, x + \phi_2 p^{m-4}] = [z, y + by'p, x(1 + ap^{m-4}) + bx'p^{m-4}]$,

(24) $[z', y' + \theta_3 p, (x' + \phi_3 p)p^{m-5}] = [z', y'(1 + dp), x(1 + dp)p^{m-5} + cxp^{m-4}]$,

in which

$$\theta_1 = d'(yz' - y'z) + x(b'z' + \beta' y'),$$

$$\theta_2 = d'yz'' + b'xz'',$$

$$\theta_3 = d'y'z'',$$

$$\phi_1 = a'xy' + \{a'(\beta' y' + b'z')\tbinom{x}{2} + a'xz + c'(yz' - y'z)\}p,$$

$$\phi_2 = a'xy'' + a'xz'' + a'b'\tbinom{x}{2}z'' + c'yz'',$$

$$\phi_3 = c'yz''.$$

A comparison of the members of the above equations give six congruences between the primed and unprimed constants and the nine indeterminates.

(I) $$\theta_1 \equiv \beta y' \pmod{p},$$

(II) $$\phi_1 \equiv ax + \beta x'p \pmod{p^2},$$

(III) $$\theta_2 \equiv by' \pmod{p},$$

(IV) $$\phi_2 \equiv ax + bx' \pmod{p},$$

(V) $$\theta_3 \equiv dy' \pmod{p},$$

(VI) $$\phi_3 \equiv cx + dx' \pmod{p}.$$

The necessary and sufficient condition for the simple isomorphism of the two groups G and G' is, *that the above congruences shall be consistent and admit of solution for the nine indeterminates, with the condition that* x, y' *and* z'' *be prime to* p.

For convenience in the discussion of these congruences, the groups are divided into six sets, and each set is subdivided into 16 cases.

The group G' is taken from the simplest case, and we associate with this case all cases, which contain a group G, simply isomorphic with G'. Then a single group G, in the selected case, simply isomorphic with G', is chosen as a type.

G' is then taken from the simplest of the remaining cases and we proceed as above until all the cases are exhausted.

Let $\kappa = \kappa_1 p^{\kappa_2}$, and $dv_1[\kappa_1, p] = 1$ ($\kappa = a, b, \alpha, \beta, c$, and d).

The six sets are given in the table below.

I.

	a_2	d_2		a_2	d_2
A	0	0	D	2	0
B	0	1	E	1	1
C	1	0	F	2	1

The subdivision into cases and the results are given in Table II.

II.

	a_2	b_2	β_2	c_2	A	B	C	D	E	F
1	1	1	1	1						
2	0	1	1	1	A_1	B_1		C_2		E_2
3	1	0	1	1	A_1		C_1	D_1		
4	1	1	0	1	A_1		C_1	D_1		E_4
5	1	1	1	0	A_1		C_1	D_1		E_5
6	0	0	1	1	A_1	B_3	C_2	C_2	E_3	F_3
7	0	1	0	1	A_1	B_4	C_2	C_2		E_7
8	0	1	1	0	A_1	B_5	C_2	C_2	E_5	E_5
9	1	0	0	1	A_1	B_3	C_1	D_1	E_3	F_3
10	1	0	1	0	A_1		C_2	C_2		E_{10}
11	1	1	0	0	A_1		*	C_1		E_{11}
12	0	0	0	1	A_1	B_3	C_2	C_2	*	E_3
13	0	0	1	0	A_1	B_{10}	*	*	E_{10}	E_{10}
14	0	1	0	0	A_1	B_{11}	C_2	C_2	E_{11}	E_{11}
15	1	0	0	0	A_1	B_{10}	C_2	C_2	E_{10}	E_{10}
16	0	0	0	0	A_1	B_{10}	*	*	E_{10}	E_{10}

The groups marked (*) divide into two or three parts.

Let $ad - bc = \theta_1 p^{\theta_2}$, $\alpha_1 d - \beta c = \phi_1 p^{\phi_2}$ and $\alpha_1 b - a\beta = \chi_1 p^{\chi_2}$ with θ_1, ϕ_1, and χ_1 prime to p.

III.

*	θ_2	ϕ_2	χ_2		*	θ_2	ϕ_2	χ_2	
C_{11}		1		D_1	D_{13}	1			D_1
C_{11}		0		C_1	D_{13}	0			C_2
C_{13}	1			C_1	D_{16}	1			C_1
C_{13}	0			C_2	D_{16}	0			C_2
C_{16}	1	1		D_1	E_{12}			1	F_3
C_{16}	1	0		C_1	E_{12}			0	E_3
C_{16}	0			C_2					

6. *Types.*

The type groups are given by equations (15), (16) and (17) with the values of the constants given in Table IV.

IV.

	a	b	α	β	c	d		a	b	α	β	c	d
A_1	0	0	1	0	0	1	E_1	0	0	p	0	0	0
B_1	0	0	1	0	0	0	E_2	1	0	p	0	0	0
B_3	0	1	1	0	0	0	E_3	0	1	p	0	0	0
B_4	0	0	1	1	0	0	E_4	0	0	p	1	0	0
B_5	0	0	1	0	1	0	E_5	0	0	p	0	1	0
B_{10}	0	1	1	0	κ	0	E_7	1	0	p	1	0	0
B_{11}	0	0	1	1	1	0	E_{10}	0	1	p	0	κ	0
C_1	0	0	p	0	0	1	E_{11}	0	0	p	1	1	0
C_2	ω	0	p	0	0	1	F_1	0	0	0	0	0	0
D_1	0	0	0	0	0	1	F_3	0	1	0	0	0	0

$\kappa = 1$, and a non-residue (mod p),
$\omega = 1, 2, \cdots, p-1$.

The congruences for three of these cases are completely analyzed as illustrations of the methods used.

B_{10}.

The congruences for this case have the special forms.

(I) $$b'xz' \equiv \beta y' \pmod p,$$

(II) $$\alpha' y' \equiv \alpha \pmod p,$$

(III) $$b'xz'' \equiv by' \pmod p,$$

(IV) $$\alpha' xy'' + \alpha' b' \binom{x}{2} z'' + c' yz'' \equiv ax + bx' \pmod p,$$

(V) $$d \equiv 0 \pmod p,$$

(VI) $$c' y' z'' \equiv cx \pmod p.$$

Since z' is unrestricted (I) gives $\beta \equiv 0$ or $\not\equiv 0 \pmod p$.

From (II) since $y' \not\equiv 0$, $\alpha \not\equiv 0 \pmod p$.

From (III) since $x, y', z'' \not\equiv 0$, $b \not\equiv 0 \pmod p$.

In (IV) $b \not\equiv 0$ and x' is contained in this congruence alone, and, therefore, a may be taken $\equiv 0$ or $\not\equiv 0 \pmod p$.

(V) gives $d \equiv 0 \pmod p$ and (VI), $c \not\equiv 0 \pmod p$.

Elimination of y' between (III) and (VI) gives

$$b'c'z''^2 \equiv bc \pmod p$$

so that bc is a quadratic residue or non-residue $(\bmod\ p)$ according as $b'c'$ is a residue or non-residue.

The types are given by placing $a = 0$, $b = 1$, $\alpha = 1$, $\beta = 0$, $c = \kappa$, and $d = 0$ where κ has the two values, 1 and a representative non-residue of p.

C_2.

The congruences for this case are

(I) $$d'(yz' - y'z) \equiv \beta y' \pmod p,$$

(II) $$\alpha_1' xy' + \alpha' xz' \equiv \alpha_1 x + \beta x' \pmod p,$$

(III) $$d' yz'' \equiv by' \pmod p,$$

(IV) $$\alpha' xz'' \equiv ax + bx' \pmod p,$$

(V) $$d' z'' \equiv d \pmod p,$$

(IV) $$cx + dx' \equiv 0 \pmod p.$$

Since z appears in (I) alone, β can be either $\equiv 0$ or $\not\equiv 0 \pmod p$. (II) is linear in z' and, therefore, $\alpha \equiv 0$ or $\not\equiv 0 \pmod p$, (III) is linear in y and, therefore, $b \equiv 0$ or $\not\equiv 0$.

Elimination of x' and z'' between (IV), (V), and (VI) gives

$$a'd^2 \equiv d'(ad - bc) \pmod{p}.$$

Since z'' is prime to p, (V) gives $d \not\equiv 0 \pmod{p}$, so that $ad - bc \not\equiv 0 \pmod{p}$. We may place $b = 0$, $\alpha = p$, $\beta = 0$, $c = 0$, $d = 1$, then a will take the values $1, 2, 3, \cdots, p-1$ giving $p - 1$ types.

D_1.

The congruences for this case are

(I) $$d'(yz' - y'z) \equiv \beta y' \pmod{p},$$

(II) $$\alpha_1 x + \beta x' \equiv 0 \pmod{p},$$

(III) $$d'yz'' \equiv by' \pmod{p},$$

(IV) $$ax + bx' \equiv 0 \pmod{p},$$

(V) $$d'z'' \equiv d \pmod{p},$$

(VI) $$cx + dx' \equiv 0 \pmod{p}.$$

z is contained in (I) alone, and therefore $\beta \equiv 0$ or $\not\equiv 0 \pmod{p}$.

(III) is linear in y, and $b \equiv 0$ or $\not\equiv 0 \pmod{p}$.

(V) gives $d \not\equiv 0 \pmod{p}$.

Elimination of x' between (II) and (VI) gives $\alpha_1 d - \beta c \equiv 0 \pmod{p}$, and between (IV) and (VI) gives $ad - bc \equiv 0 \pmod{p}$. The type group is derived by placing $a = 0$, $b = 0$, $\alpha = 0$, $\beta = 0$, $c = 0$ and $d = 1$.

Section 2.

1. *Groups with dependent generators.* In this section, G is generated by Q_1 and P where

(1) $$Q_1^{p^2} = P^{hp^2}.$$

There is in G, a subgroup H_1, of order p^{m-2}, which contains $\{P\}$ self-conjugately.* H_1 either contains, or does not contain Q_1^p. We will consider the second possibility in the present section, reserving the first for the next section.

2. *Determination of* H_1. H_1 is generated by P and some other operator R_1 of G. R_1^p is contained in $\{P\}$. Let

(2) $$R_1^p = P^{lp}.$$

Since $\{P\}$ is self-conjugate in H_1,

* BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

(3) $$R_1^{-1}PR_1 = P^{1+kp^{m-4}}\dagger$$

Denoting $R_1^a P^b R_1^c P^d \cdots$ by the symbol $[a, b, c, d, \cdots]$ we derive from (3)

(4) $$[-y, x, y] = [0, x(1+kyp^{m-4})] \qquad (m>4),$$

and

(5) $$[y, x]^s = [sy, x\{s + k\tbinom{s}{2}yp^{m-4}\}]$$

Placing $s = p$ and $y = 1$ in (5) we have, from (2)

$$[R_1 P^x]^p = R_1^p P^{xp} = P^{(l+x)p}.$$

Choosing x so that

$$x + l \equiv 0 \pmod{p^{m-4}},$$

$R = R_1 P^x$ is an operator of order p, which will be used in the place of R_1, and $H_1 = \{R, P\}$ with $R^p = 1$.

3. *Determination of H_2.* We will now use the symbol $[a, b, c, d, e, f, \cdots]$ to denote $Q_1^a R^b P^c Q_1^d R^e P^f \cdots$.

H_1 and Q_1 generate G and all the operations of G are given by $[z, y, x]$ ($z=0, 1, 2, \cdots, p^2-1$; $y=0, 1, 2, \cdots, p-1$; $x=0, 1, 2, \cdots, p^{m-3}-1$), since these are p^m in number and are all distinct. There is in G a subgroup H_2 of order p^{m-1} which contains H_1 self-conjugately. H_2 is generated by H_1 and some operator $[z, y, x]$ of G. Q_1^z is then in H_2 and H_2 is the subgroup $\{Q_1^p, H_1\}$. Hence,

(6) $$Q_1^{-p}PQ_1^p = R^\beta P^{a_1},$$

(7) $$Q_1^{-p}PQ_1^p = R^{b_1}P^{ap^{m-4}}.$$

To determine a_1 and β we find from (6), (5) and (7)

$$[-p^2, 0, 1, p^2] = \left[0, \frac{a_1^p - b_1^p}{a_1 - b_1}\beta, a_1^p\left\{1 + \frac{\beta k}{2}\frac{a_1^p - 1}{a_1 - 1}p^{m-4}\right\}\right.$$
$$\left. + a\beta\left\{p\frac{a_1^{p-1}}{a_1 - b_1} - \frac{a_1^p - b_1^p}{(a_1 - b_1)^2}\right\}p^{m-4}\right].$$

By (1)

$$Q_1^{-p^2}PQ_1^{p^2} = P,$$

and, therefore,

$$\frac{a_1^p - b_1^p}{a_1 - b_1}\beta \equiv 0 \pmod{p},$$

$$a_1^p \equiv 1 \pmod{p^{m-4}}, \qquad \text{and} \qquad a_1 \equiv 1 \pmod{p^{m-5}} \quad (m>5).$$

Let $a_1 = 1 + a_2 p^{m-5}$ and equation (6) is replaced by

(8) $$Q_1^{-p}PQ_1^p = R^\beta P^{1+a_2p^{m-5}}.$$

† BURNSIDE, *Theory of Groups*, Art. 56, p. 66.

To find a and b_1, we obtain from (7), (8) and (5)

$$[-p^2, 1, 0, p^2] = \left[0, b_1^p, a\frac{b_1^p - 1}{b_1 - 1}p^{m-4}\right].$$

By (1) and (4)

$$Q_1^{-p^2} R Q_1^{p^2} = P^{-lp^2} R P^{lp^2} = R,$$

and, hence,

$$b_1^p \equiv 1 \pmod{p}, \qquad a\frac{b_1^p - 1}{b_1 - 1} \equiv 0 \pmod{p},$$

therefore $b_1 = 1$.

Substituting $b_1 = 1$ and $\alpha_1 = 1 + \alpha_2 p^{m-5}$ in the congruence determining α_1 we obtain $(1 + \alpha_2 p^{m-5})^p \equiv 1 \pmod{p^{m-3}}$, which gives $\alpha_2 \equiv 0 \pmod{p}$.

Let $\alpha_2 = ap$ and equations (8) and (7) are now replaced by

$$Q_1^p P Q_1^p = R^\beta P^{1+ap^{m-4}}, \tag{9}$$

$$Q_1^{-p} R Q_1^p = R P^{ap^{m-4}}. \tag{10}$$

From these we derive

(11) $[-yp, 0, x, yp] = [0, \beta xy, x + \{axy + a\beta x\binom{y}{2} + \beta k\binom{x}{2}y\}p^{m-4}]$,

(12) $[-yp, x, 0, yp] = [0, x, axyp^{m-4}]$.

A continued use of (4), (11), and (12) yields

$$[zp, y, x]^s = [szp, sy + U_s, sx + V_s p^{m-4}] \tag{13}$$

where

$$U_s = \beta\binom{s}{2}xz,$$

$$V_s = \binom{s}{2}\{axz + \beta k\binom{x}{2}z + kxy + ayz\} + \beta k\binom{s}{3}x^2 z$$
$$+ \tfrac{1}{2}a\beta\{\tfrac{1}{3!}s(s-1)(2s-1)z^2 - \binom{s}{2}z\}.$$

4. *Determination of G.*

Since H_2 is self-conjugate in G_1 we have

$$Q_1^{-1} P Q_1 = Q_1^{\gamma p} R^\delta P^{\epsilon_1}, \tag{14}$$

$$Q_1^{-1} R Q_1 = Q_1^{c p} R^d P^{e p^{m-4}}. \tag{15}$$

From (14), (15) and (13)

$$[-p, 0, 1, p] = [\lambda p, \mu, \epsilon_1^p + \nu p^{m-4}]$$

and by (9) and (1)

$$\lambda p \equiv 0 \pmod{p^2},$$

$$\epsilon_1^p + \nu p^{m-4} + \lambda h p \equiv 1 + a p^{m-4} \pmod{p^{m-3}}.$$

from which

$$\epsilon_1^p \equiv 1 \pmod{p^2}, \text{ and } \epsilon_1 \equiv 1 \pmod{p} \qquad (m>5).$$

Let $\epsilon_1 = 1 + \epsilon_2 p$ and equation (14) is replaced by

(16) $$Q_1^{-1} P Q_1 = Q_1^{\gamma p} R^{\delta} P^{1+\epsilon_2 p}.$$

From (15), (16), and (13)

$$[-p, 1, 0, p] = \left[c\frac{d^p - 1}{d-1}p, d^p, Kp^{m-4}\right]$$

where

$$K = \frac{d^p - 1}{d-1}e + \sum_1^{p-1} acd\frac{d^n(d^n-1)}{2}.$$

By (10)

$$d^p \equiv 1 \pmod{p}, \text{ and } d = 1$$

and by (1)

$$chp^2 \equiv ap^{m-4} \pmod{p^{m-3}}.$$

Equation (15) is now replaced by

(17) $$Q_1^{-1} R Q_1 = Q_1^{cp} R P^{ep^{m-4}}.$$

A combination of (17), (16) and (13) gives

$$[-p, 0, 1, p] = \left[\left\{\gamma\frac{(1+\epsilon_2 p)^p - 1}{\epsilon_2 p^2} + c\delta\frac{p-1}{2}\right\}p^2, 0, (1+\epsilon_2 p)^p\right].$$

By (9)

$$\left\{\gamma\frac{(1+\epsilon_2 p)^p - 1}{\epsilon_2 p^2} + c\delta\frac{p-1}{2}\right\}hp^2 + (1+\epsilon_2 p)^p \equiv 1 + ap^{m-4} \pmod{p^{m-3}},$$

$\beta \equiv 0 \pmod{p}$.

A reduction of the first congruence gives

$$\frac{(1+\epsilon_2 p)^p - 1}{\epsilon p^2}\{\epsilon_2 + \gamma h\}p^2 \equiv \left\{a - a\delta\frac{p-1}{2}\right\}p^{m-4} \pmod{p^{m-3}}$$

and, since

$$\frac{(1+\epsilon_2 p)^p - 1}{\epsilon_2 p^2} \equiv 1 \pmod{p}, \qquad (\epsilon_2 + \gamma h)p^2 \equiv 0 \pmod{p^{m-4}}$$

and

$$(18) \qquad (\epsilon_2 + \gamma h)p^2 \equiv \left(\alpha + \frac{a\,\delta}{2}\right)p^{m-4} \pmod{p^{m-3}}.$$

From (17), (16), (13) and (18)

$$(19) \quad [-y, x, 0, y] = [cxyp, x, \{exy + ac\tbinom{x}{2}y\}p^{m-4}],$$

$$(20) \quad [-y, 0, x, y] = [x\{\gamma y + c\delta\tbinom{y}{2}\}p, \delta xy, x(1+\epsilon_2 yp) + \theta p^{m-4}]$$

where

$$\theta = \{e\delta x + a\delta\gamma x + \epsilon_2\left(\alpha + \frac{a\,\delta}{2}\right)x\}\tbinom{y}{2} + \tfrac{1}{2}ac\{\tfrac{1}{3!}y(y-1)(2y-1)\delta^2 - \tbinom{y}{2}\delta\} + \{\alpha\gamma y + \delta ky + a\delta xy^2 + (ac\delta^2 y + ac\delta)\tbinom{y}{2}\}\tbinom{x}{2}.$$

From (19), (20), (4) and (18)

$$\{Q_1P^x\}^{p^2} = Q_1^{p^2}P^{xp^2} = P^{(h+x)p^2}.$$

If x be so chosen that

$$h + x \equiv 0 \pmod{p^{m-5}}$$

$Q = Q_1P^x$ is an operator of order p^2 which will be used in place Q_1 and $Q^{p^2} = 1$.

Placing $h = 0$ in (18) we get

$$\epsilon_2 p^2 \equiv 0 \pmod{p^{m-4}}.$$

Let $\epsilon_2 = \epsilon p^{m-6}$ and equation (16) is replaced by

$$(21) \qquad Q^{-1}PQ = Q^{\gamma p}R^{\delta}P^{1+\epsilon p^{m-5}}$$

The congruence

$$ap^{m-4} \equiv chp^2 \pmod{p^{m-3}}$$

becomes

$$ap^{m-4} \equiv 0 \pmod{p^{m-3}}, \qquad \text{and} \qquad a \equiv 0 \pmod{p}.$$

Equations (19) and (20) are replaced by

$$(22) \quad [-y, x, 0, y] = [cxyp, x, exyp^{m-4}]$$

$$(23) \quad [-y, 0, x, y] = [\{\gamma y + c\delta\tbinom{y}{2}\}xp, \delta xy, x(1+\epsilon yp^{m-5}) + \theta p^{m-4}]$$

where

$$\theta = e\delta x\tbinom{y}{2} + \{\alpha\gamma y + \delta ky + \alpha c\delta\tbinom{y}{2}\}\tbinom{x}{2}.$$

A formula for any power of an operation of G is derived from (4), (22) and (23)

$$(24)\qquad [z, y, x]^s = [sz + U_s p,\ sy + V_s,\ sx + W_s p^{m-5}]$$

where

$$U_s = \binom{s}{2}\{\gamma xz + cyz\} + \tfrac{1}{2}c\delta x\{\tfrac{1}{3!}s(s-1)(2s-1)z^2 - \binom{s}{2}z\},$$

$$V_s = \delta\binom{s}{2}xz,$$

$$W_s = \binom{s}{2}\{exz + [(a\gamma+\delta k)\binom{x}{2}z + eyz + kxy]\,p\} + \binom{s}{3}\{\epsilon\gamma x + \epsilon y + \delta kx\}xzp$$

$$+\tfrac{1}{2}c\delta\epsilon\{\tfrac{1}{2}(s-1)z^2 - z\}\binom{s}{3}xp + \tfrac{1}{2}\{\delta ex + ac\delta\binom{x}{2}\}\{\tfrac{1}{3!}s(s-1)(2s-1)z^2 - \binom{s}{2}z\}p.$$

5. *Transformations of the groups.* Placing $y = 1$ and $x = -1$ in (22) we obtain (17) in the form

$$R^{-1}QR = Q^{1-cp}P^{-ep^{m-4}}.$$

A comparison of the generational equations of the present section with those of Section 1, shows that groups, in which $\delta \equiv 0 \pmod p$, are simply isomorphic with those in Section 1, so we need consider only those cases in which $\delta \not\equiv 0 \pmod p$.

All groups of this section are given by

$$G:\ \begin{cases} R^{-1}PR = P^{1+kp^{m-4}}, & (25)\\ Q^{-1}PQ = Q^{\gamma p}R^{\delta}P^{1+\epsilon p^{m-5}}. & (26)\\ Q^{-1}RQ = Q^{cp}RP^{ep^{m-4}}. & (27)\end{cases}$$

$R^p = 1$, $Q^{p^2} = 1$, and $P^{p^{m-3}} = 1$, $(k, \gamma, c, e = 0, 1, 2, \cdots, p-1;$ $\delta = 1, 2, \cdots, p-1;$ $\epsilon = 0, 1, 2, \cdots, p^2 - 1)$.

Not all these groups, however, are distinct. Suppose that G and G' of the above set are simply isomorphic and that the correspondence is given by

$$C = \begin{bmatrix} R, & Q, & P \\ R_1', & Q_1', & P_1' \end{bmatrix}.$$

Since $R^p = 1$, $Q^{p^2} = 1$, and $P^{p^{m-3}} = 1$, $R_1'^p = 1$, $Q_1'^{p^2} = 1$ and $P_1'^{p^{m-3}}$. The forms of these operators are then

$$P_1' = Q'^zR'^yP'^x,$$

$$R_1' = Q'^{z'p}R'^{y'}P'^{x'p^{m-4}},$$

$$Q_1' = Q'^{z''}R'^{y''}P'^{x''p^{m-5}},$$

where $dv[x, p] = 1$.

Since R is not contained in $\{P\}$, and Q^p is not contained in $\{R, P\}$ R'_1 is not contained in $\{P'_1\}$, and Q'^p_1 is not contained in $\{R'_1, P'_1\}$.

Let

$$R'^{s'}_1 = P'^{sp^{m-4}}_1.$$

This becomes in terms of Q', R' and P'

$$[s'z'p, s'y', s'x'p^{m-4}] = [0, 0, sxp^{m-4}],$$

and

$$s'y' \equiv 0 \pmod{p}, \qquad s'z' \equiv 0 \pmod{p}.$$

Either y' or z' is prime to p or s' may be taken $= 1$.

Let

$$Q'^{s''p}_1 = R'^{s'}_1 P'^{sp^{m-4}}_1,$$

and in terms of Q', R' and P'

$$[s''z''p, 0, s''x''p^{m-4}] = [s'z'p, s'y', (s'x' + sx)p^{m-4}],$$

from which

$$s''z'' \equiv s'z' \pmod{p}, \qquad \text{and} \qquad s'y' \equiv 0 \pmod{p}.$$

Eliminating s' we find

$$s''y'z'' \equiv 0 \pmod{p},$$

$dv[y'z'', p] = 1$ or s'' may be taken $= 1$. We have then z'', y' and x *prime to* p.

Since R, Q and P satisfy equations (25), (26) and (27) R'_1, Q'_1 and P'_1 do also. These become in terms of R', Q' and P'.

$$[z + \Phi'_1 p, y, x + \Theta'_1 p^{m-4}] = [z, y, x(1 + kp^{m-4})],$$

$$[z + \Phi'_2 p, y + \delta' x z'', x + \Theta'_2 p^{m-5}] = [z + \Phi_2 p, y + \delta y', x + \Theta_2 p^{m-5}],$$

$$[(z' + \Phi'_3)p, y', \Theta'_3 p^{m-4}] = [(z' + \Phi_3)p, y, \Theta'_3 p^{m-4}],$$

where

$$\Phi'_1 = -c'yz', \qquad \Theta'_1 = \epsilon' x z' + k' x y' - e' y' z,$$

$$\Phi'_2 = \{\gamma' z'' + c'\delta'\tbinom{z}{2}\} x + c'(yz'' - y''z),$$

$$\Theta'_2 = \epsilon' x z'' + \{\tbinom{x}{2}[\alpha'\gamma' z'' + \alpha' c'\delta'\tbinom{z''}{2}) + \delta' k' z''] + \delta' e' x\tbinom{z''}{2}$$
$$+ e'(yz'' - y''z) + k' x y''\} p,$$

$$\Phi_2 = \gamma z'' + \delta z' + c'\delta y' z, \qquad \Theta_2 \equiv \epsilon x + (\gamma x'' + \delta x + e'\delta y' z)p,$$

$$\Phi'_3 = c'y'z'', \qquad \Theta'_3 = e'y'z'', \qquad \Phi_3 = cz'', \qquad \Theta_3 = ex + cx''.$$

A comparison of the members of these equations give seven congruences

(I) $$\Phi_1' \equiv 0 \pmod{p},$$

(II) $$\Theta_1' \equiv kx \pmod{p},$$

III) $$\Phi_2' \equiv \Phi_2 \pmod{p}.$$

(IV) $$\delta' x z'' \equiv \delta y' \pmod{p},$$

(V) $$\Theta_2' \equiv \Theta_2 \pmod{p^2},$$

(VI) $$\Phi_3' \equiv c z'' \pmod{p},$$

(VII) $$\Theta_3' \equiv \Theta_3 \pmod{p}.$$

The necessary and sufficient condition for the simple isomorphism of G and G' is, *that these congruences be consistent and admit of solution for the nine indeterminants with x, y', and z'' prime to p.*

Let $\kappa = \kappa_1 p^{\kappa_2}$, $dv[\kappa_1, p] = 1$ $(\kappa = k, \delta, \gamma, \epsilon, c, e)$.

The groups are divided into three parts and each part is subdivided into 16 cases.

The methods used in discussing the congruences are the same as those used in Section 1.

6. *Reduction to types.* The three parts are given by

I.

	ϵ_2	δ_2
A	0	0
B	1	0
C	2	0

The subdivision into cases and the results of the discussion of the congruences are given in Table II.

II.

	k_2	γ_2	c_2	e_2	A	B	C
1	1	1	1	1			B_1
2	0	1	1	1			B_2
3	1	0	1	1	A_2	B_1	B_1
4	1	1	0	1			B_4
5	1	1	1	0			B_5
6	0	0	1	1	*	B_2	B_2
7	0	1	0	1	A_4		B_7
8	0	1	1	0	A_5	B_5	B_5
9	1	0	0	1	A_4	B_4	B_4
10	1	0	1	0	A_5	B_5	B_5
11	1	1	0	0	A_4	B_4	B_4
12	0	0	0	1	A_4	B_7	B_7
13	0	0	1	0	A_5	B_5	B_5
14	0	1	0	0	A_4	B_7	B_7
15	1	0	0	0	A_4	B_4	B_4
16	0	0	0	0	A_4	B_7	B_7

A_6 divides into two parts.

The groups of A_6 in which $\delta k + \epsilon\gamma \equiv 0 \pmod{p}$ are simply isomorphic with the groups of A_1 and those in which $\delta k + \epsilon\gamma \not\equiv 0 \pmod{p}$ are simply isomorphic with the groups of A_2. The types are given by equations (25), (26) and (27) where the constants have the values given in Table III.

III.

	k	δ	γ	ϵ	c	e
A_1	0	1	0	1	0	0
A_2	1	1	0	1	0	0
A_4	0	1	0	1	1	0
A_5	0	1	0	1	0	ω
B_1	0	1	0	p	0	0
B_2	1	1	0	p	0	0
B_4	0	1	0	p	1	0
B_5	0	1	0	p	0	κ
B_7	1	1	0	p	ω	0

$\kappa = 1$, and a non-residue $(\text{mod}\, p)$,
$\omega = 1, 2, \cdots, p-1$.

A detailed analysis of several cases is given below, as a general illustration of the methods used.

A_1.

The special forms of the congruences for this case are

(II) $$\epsilon' x z' \equiv kx \pmod{p},$$

(III) $$\gamma z'' + \delta z' \equiv 0 \pmod{p},$$

(IV) $$\delta' x z'' \equiv \delta y' \pmod{p},$$

(V) $$\epsilon' x z'' \equiv e x \pmod{p},$$

(VI) $$c z'' \equiv 0 \pmod{p},$$

(VII) $$e x \equiv 0 \pmod{p}.$$

Congruence (IV) gives $\delta \not\equiv 0 \pmod{p}$, from (II) k can be $\equiv 0$ or $\not\equiv 0 \pmod{p}$, III gives $\gamma \equiv 0$ or $\not\equiv 0$, (V) gives $\epsilon \not\equiv 0$, (VI) and (VII) give $c \equiv e \equiv 0 \pmod{p}$. Elimination of x, z' and z'' between (II), (III) and (V) gives $\delta k + \gamma\epsilon \equiv 0 \pmod{p}$. If $k \equiv 0$, then $\gamma \equiv 0 \pmod{p}$ and if $k \not\equiv 0$, then $\gamma \not\equiv 0 \pmod{p}$.

A_2.

The congruences for this case are

(II) $$\epsilon' x z' + k' x y' \equiv k x \pmod{p},$$

(III) $$\gamma z'' + \delta z' \equiv 0 \pmod{p},$$

(IV) $$\delta' x z'' \equiv \delta y' \pmod{p},$$

(V) $$\epsilon' x z'' \equiv \epsilon x \pmod{p},$$

(VI) $$c z'' \equiv 0 \pmod{p},$$

(VII) $$e x \equiv 0 \pmod{p}.$$

Congruence (III) gives $\gamma \equiv 0$ or $\not\equiv 0$, (IV) gives $\delta \not\equiv 0$, (V) $\epsilon \not\equiv 0$, (VI) and (VII) give $c \equiv e \equiv 0 \pmod{p}$. Elimination of x, z', and z'' between (II), (III) and (V) gives

$$\delta k + \gamma \epsilon \equiv k' \delta y' \pmod{p}$$

from which

$$\delta k + \gamma \epsilon \not\equiv 0 \pmod{p}.$$

If $k \equiv 0$, then $\gamma \not\equiv 0$, and if $\gamma \equiv 0$ then $k \not\equiv 0 \pmod{p}$.

Both γ and k can be $\not\equiv 0 \pmod{p}$ provided the above condition is fulfilled.

A_5.

The congruences for this case are

(II) $$\epsilon' x z' - e' y' z \equiv k x \pmod{p},$$

(III) $$\gamma z'' + \delta z' \equiv 0 \pmod{p},$$

(IV) $$\delta' x z'' \equiv \delta y' \pmod{p},$$

(V) $$\epsilon' x z'' \equiv \epsilon x \pmod{p},$$

(VI) $$c z'' \equiv 0 \pmod{p},$$

(VII) $$e' y' z'' \equiv e x \pmod{p}.$$

(II) and (III) are linear in z and z' so k and γ are $\equiv$ or $\not\equiv 0 \pmod{p}$ independently, (IV) gives $\delta \not\equiv 0$, (V) give $\epsilon \not\equiv 0$, (VI) $c \equiv 0$, and (VII) $e \not\equiv 0$.

Elimination between (IV), (V), and (VII) gives

$$\delta' e' \epsilon^2 \equiv \delta e \epsilon'^2 \pmod{p}.$$

The types are derived by placing $\epsilon = \delta = 1$, and $e = 1, 2, \cdots, p-1$.

B_5.

The congruences for this case are

(II) $$-e'y'z \equiv kx \pmod p,$$

(III) $$\gamma z'' + \delta z' \equiv 0 \pmod p,$$

(IV) $$\delta' x z'' \equiv \delta y' \pmod p,$$

(V) $$\epsilon_1' x z'' + \delta' e' x \binom{z''}{2} + e' y z'' \equiv \epsilon_1 x + \gamma x'' + \delta x' \pmod p,$$

(VI) $$c z'' \equiv 0 \pmod p,$$

(VII) $$e'y'z'' \equiv ex \pmod p.$$

(II), and (III) being linear in z and z' give $k \equiv 0$ or $\not\equiv 0$, and $\gamma \equiv 0$ or $\not\equiv 0 \pmod p$, (IV) gives $\delta \not\equiv 0$, (V) being linear in x' gives $\epsilon_1 \equiv 0$ or $\not\equiv 0 \pmod p$, (VI) gives $c \equiv 0$ and (VII) $e \not\equiv 0$.

Elimination of x and y' from (IV) and (VII) gives

$$\delta' e' z''^2 \equiv \delta e \pmod p.$$

δe is a quadratic residue or non-residue $(\mathrm{mod}\ p)$ according as $\delta' e'$ is a residue or non-residue.

The two types are given by placing $\delta = 1$, and $e = 1$ and a non-residue $(\mathrm{mod}\ p)$.

Section 3.

1. *Groups with dependent generators continued.* As in Section 2, G is here generated by Q_1 and P, where

$$Q_1^{p^2} = P^{hp^2}.$$

Q_1^p is contained in the subgroup H_1 of order p^{m-2}, $H_1 = \{Q_1^p, P\}$.

2. *Determination of* H_1. Since $\{P\}$ is self-conjugate in H_1

(1) $$Q_1^{-p} P Q_1^p = P^{1+kp^{m-4}}.$$

Denoting $Q_1^a P^b Q_1^c P^d \cdots$ by the symbol $[a, b, c, d, \cdots]$, we have from (1)

(2) $$[-yp, x, yp] = [0, x(1 + kyp^{m-4})] \qquad (m > 4).$$

Repeated multiplication with (2) gives

(3) $$[yp, x]^s = [syp, x\{s + k\tbinom{s}{2} yp^{m-4}\}].$$

3. *Determination of* H_2. There is a subgroup H_2 of order p^{m-1} which contains H_1 self-conjugately.* H_2 is generated by H_1 and some operator

* Burnside, *Theory of Groups*, Art. 54, p. 64.

R_1 of G. R_1^p is contained in H_1, in fact in $\{P\}$, since if $R_1^{p^2}$ is the first power of R_1 in $\{P\}$, then $H_2 = \{R_1, P\}$, which case was treated in Section 1.

(4) $$R_1^p = P^{lp}.$$

Since H_1 is self-conjugate in H_2

(5) $$R_1^{-1} P R_1 = Q_1^{\beta p} P^{a_1}.$$

(6) $$R_1^{-1} Q^p R_1 = Q_1^{bp} P^{a_1 p}.$$

Using the symbol $[a, b, c, d, e, f, \cdots]$ to denote $R_1^a Q_1^b P^c R_1^d Q_1^e P^f \cdots$, we have from (5), (6) and (3)

(7) $$[-p, 0, 1, p] = [0, \beta N p, a_1^p + Mp],$$

and by (4)

$$a_1^p \equiv 1 \pmod p, \qquad \text{and} \qquad a_1 \equiv 1 \pmod p.$$

Let $a_1 = 1 + a_2 p$ and (5) is now replaced by

(8) $$R_1^{-1} P R_1 = Q_1^{\beta p} P^{1 + a_2 p}.$$

From (6), (8) and (3)

$$[-p, p, 0, p] = [0, b^p p, a_1 \frac{b^p - 1}{b - 1} p + a_1 U p^2],$$

and by (4) and (2)

$$R_1^{-p} Q_1^p R_1^p = Q_1^p$$

and therefore $b^p \equiv 1 \pmod p$, and $b = 1$. Placing $b = 1$ in the above equation the exponent of P takes the form

$$a_1 p^2 (1 + U' p) = a_1 \frac{\{1 + (a_2 + \beta h) p\}^p - 1}{(a_2 + \beta h) p^2} p^2$$

from which

$$a_1 p^2 (1 + U' p) \equiv 0 \pmod{p^{m-3}}$$

or

$$a_1 \equiv 0 \pmod{p^{m-5}} \qquad (m > 5).$$

Let $a_1 = a p^{m-5}$ and (6) is replaced by

(9) $$R_1^{-1} Q_1^p R_1 = Q_1^p P^{a p^{m-4}}.$$

(7) now has the form

$$[-p, 0, 1, p] = [0, \beta N p, (1 + a_2 p)^p + M p^2],$$

where

$$N = p \text{ and } M = \beta h \left\{ \frac{(1 + a_2 p)^p - 1}{a_2 p^2} - 1 \right\},$$

from which

$$(1+\alpha_2 p)^p + \frac{(1+\alpha_2 p)^p - 1}{\alpha_2 p^2}\beta h p^2 \equiv 1 \pmod{p^{m-3}}$$

or

$$\frac{(1+\alpha_2 p)^p - 1}{\alpha_2 p^2}\{\alpha_2 + \beta h\} p^2 \equiv 0 \pmod{p^{m-3}}$$

and since

$$\frac{(1+\alpha_2 p)^p - 1}{\alpha_2 p^2} \equiv 1 \pmod{p}$$

(10) $$(\alpha_2 + \beta h)p^2 \equiv 0 \pmod{p^{m-3}}.$$

From (8), (9), (10) and (3)

(11) $$[-y, 0, x, y] = [0, \beta xyp, x(1+\alpha_2 yp) + \theta p^{m-4}],$$

(12) $$[-y, xp, 0, y] = [0, xp, axyp^{m-4}],$$

where

$$\theta = a\beta x\binom{y}{2} + \beta k\binom{x}{2}y.$$

By continued use of (11), (12), (2) and (10)

(13) $$[z, yp, x]^s = [sz, (sy + U_s)p, xs + V_s p],$$

where

$$U_s = \beta\binom{s}{2}xz$$

$$V_s = \binom{s}{2}\{\alpha_2 xz + [ayz + kxy + \beta k\binom{x}{2}z]p^{m-5}\}$$
$$+ \{\beta\binom{s}{3}x^2 z + \tfrac{1}{2}a\beta[\tfrac{1}{3!}s(s-1)(2s-1)z^2 - \binom{s}{2}z]x\}p^{m-5}$$

Placing in this $y = 0$, $z = 1$ and $s = p$,

$$(R_1 P^x)^p = R_1^p P^{xp} = P^{(x+l)p},\text{*}$$

determine x so that

$$x + l \equiv 0 \pmod{p^{m-4}},$$

then $R = R_1 P^x$ is an operator of order p which will be used in the place of R_1, $R^p = 1$.

4. *Determination of G.* Since H_2 is self-conjugate in G

(14) $$Q_1^{-1} P Q_1 = R^\gamma Q_1^{\delta p} P^{\epsilon_1},$$

(15) $$Q_1^{-1} R Q_1 = R^c Q_1^{dp} P^{e_1 p}.$$

---

* Terms of the form $(Ax^2 + Bx)p^{m-4}$ in the exponent of P for $p = 3$ and $m > 5$ do not alter the result.

From (15)

$$(R^c Q_1^{dp} P^{e_1 p})^p = 1,$$

by (13)

$$Q_1^{lp^2} P^{e_1 p^2} = P^{(e_1+dh)p^2} = 1,$$

and

(16) $$(e_1 + dh)p^2 \equiv 0 \pmod{p^{m-3}}.$$

From (14), (15) and (13)

(17) $$[0, -p, 1, 0, p] = [L, Mp, \epsilon_1^p + Np].$$

By (1)

$$\epsilon_1^p \equiv 1 \pmod{p}, \qquad \text{and} \qquad \epsilon_1 \equiv 1 \pmod{p}.$$

Let $\epsilon_1 = 1 + \epsilon_2 p$ and (14) is replaced by

(18) $$Q_1^{-1} P Q_1 = R^\gamma Q_1^{\delta p} P^{1+\epsilon_2 p}.$$

From (15), (18), and (13)

$$[0, -p, 0, 1, p] = \left[c^p, \frac{c^p - 1}{c - 1} dp, Kp\right].$$

Placing $x = 1$ and $y = -1$ in (12) we have

(19) $$[0, -p, 0, 1, p] = [1, 0, -ap^{m-4}],$$

and therefore $c^p \equiv 1 \pmod{p}$, and $c = 1$. (15) is now replaced by

(20) $$Q_1^{-1} R Q_1 = R Q_1^{dp} P^{e_1 p}.$$

Substituting $1 + \epsilon_2 p$ for ϵ_1 and 1 for c in (17) gives, by (16)

$$[0, -p, 1, p] = [0, Mp^2, (1 + \epsilon_2 p)^p + Np^2],$$

where

$$M = \gamma d \frac{p-1}{2} + \delta \frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2}$$

and

$$N = \frac{e_1 \gamma}{(\epsilon_2 + \delta h)p^2} \left\{ \frac{[1 + (\epsilon_2 + \delta h)p]^p - 1}{(\epsilon_2 + \delta h)p} - p \right\}.$$

By (1)

$$(1 + \epsilon_2 p)^p + (N + Mh)p^2 \equiv 1 + kp^{m-4} \pmod{p^{m-3}},$$

or reducing

$$\psi(\epsilon_2 + \delta h)p^2 \equiv kp^{m-4} \pmod{p^{m-3}},$$

where

$$\psi = \frac{(1 + \epsilon_2 p)^p - 1}{\epsilon_2 p^2} + N - e_1 \gamma \frac{p-1}{2}.$$

Since

$$\psi \equiv 1 \pmod{p}.$$

(21) $$(\epsilon_2 + \delta h)p^2 \equiv kp^{m-4} \pmod{p^{m-3}}.$$

From (18), (20), (13), (16) and (21)

(22) $$[0, -y, x, 0, y] = [\gamma xy, \theta_1 p, x + \phi_1 p],$$

(23) $$[0, -y, 0, x, y] = [x, dxyp, \phi_2 p],$$

where

$$\theta_1 = d\gamma x\binom{y}{2} + \delta xy + \beta\gamma\binom{x}{2}y,$$

$$\phi_1 = \epsilon_2 xy + \alpha_2\gamma\binom{x}{2}y + e_1\gamma\binom{y}{2}x + \{x\binom{y}{2}(\epsilon_2 k + \delta\gamma)$$
$$+\tfrac{1}{2}ad\left[\tfrac{1}{3!}y(y-1)(2y-1)\gamma^2 - \binom{y}{2}\gamma\right]x + a\gamma^2 dx\tfrac{1}{3!}y(y+1)(y-1)$$
$$+ e_1\gamma k\binom{y}{3}x + \tfrac{1}{2}a\beta\left[\tfrac{1}{3!}x(x-1)(2x-1)\gamma^2 y^2 - \binom{x}{2}\gamma y\right]$$
$$+ \binom{x}{2}(a+k)\left[dy\binom{y}{2} + \delta y\right] + \beta\gamma\binom{x}{3}\}p^{m-5},$$

$$\phi_2 = e_1 xy + \{e_1 k\binom{y}{2} + ad\binom{x}{2}y\}p^{m-5}.$$

Placing $x = 1$ and $y = p$ in (23) and by (16)

$$Q_1^{-p}RQ_1^p = R,$$

and by (19)

$$a \equiv 0 \pmod{p}.$$

A continued multiplication, with (11), (22), and (23), gives

$$(Q_1 P^x)^{p^2} = Q_1^{p^2}P^{xp^2} = P^{(x+l)p^2}.$$

Let x be so chosen that

$$(x + l) \equiv 0 \pmod{p^{m-5}},$$

then $Q = Q_1 P^x$ is an operator of order p^2 which will be used in place of Q_1, $Q^{p^2} = 1$, and

$$h \equiv 0 \pmod{p^{m-5}}.$$

From (21), (10) and (16)

$$\epsilon_2 p^2 \equiv kp^{m-4}, \qquad \alpha_2 p^2 \equiv 0 \qquad \text{and} \qquad e_1 p^2 \equiv 0 \pmod{p^{m-3}}.$$

Let $\epsilon_2 = \epsilon p^{m-6}$, $\alpha_2 = \alpha p^{m-6}$ and $e_1 = ep^{m-5}$. Then equations (18), (20) and (8) are replaced by

$$G: \begin{cases} Q^{-1}PQ = R^{\gamma}Q^{\delta p}P^{1+\epsilon p^{m-5}}, & (24)\\ Q^{-1}RQ = RQ^{dp}P^{ep^{m-4}}, & (25)\\ R^{-1}PR = Q^{\beta p}P^{1+\alpha p^{m-4}}, & (26)\end{cases}$$

$$R^p = 1, \qquad Q^{p^2} = 1, \qquad P^{p^{m-3}} = 1.$$

(11), (22) and (23) are replaced by

$$[-y, 0, x, y] = [0, \beta xyp, x + \phi p^{m-4}], \tag{27}$$

$$[0, -y, x, 0, y] = [\gamma xy, \theta_1 p, x + \phi_1 p^{m-5}], \tag{28}$$

$$[0, -y, 0, x, y] = [x, dxyp, \phi_2 p^{m-4}], \tag{29}$$

where

$$\phi = \alpha xy + \beta k\tbinom{x}{2}y, \qquad \theta_1 = d\gamma\tbinom{y}{2}x + \delta xy + \beta\gamma\tbinom{x}{2}y,$$

$$\phi_1 = \epsilon xy + \{e\gamma x\tbinom{y}{2} + \tbinom{x}{2}(\alpha\gamma y + d\gamma k\tbinom{y}{2} + \delta ky) + \beta\gamma y\tbinom{x}{3}\}\,p,$$

$$\phi_2 = exy.$$

A formula for a general power of any operator of G is derived from (27), (28) and (29)

$$[0, z, 0, y, 0, x]^s = [0, sz + U_s p, 0, sy + V_s, 0, sx + W_s p^{m-5}], \tag{30}$$

where

$$U_s = \tbinom{s}{2}\{\delta xz + dyz + \beta xy + \beta\gamma\tbinom{x}{2}z\}$$
$$+ \tfrac{1}{2}dx\{\tfrac{1}{3!}s(s-1)(2s-1)z^2 - \tbinom{s}{2}z\}x + \beta\gamma\tbinom{s}{2}x^2z,$$
$$V_s = \gamma\tbinom{s}{2}xz,$$

$$W_s = \tbinom{s}{2}\{\epsilon xz + [\alpha xy + eyz + (\beta ky + \alpha\beta\gamma + \delta kz)\tbinom{x}{2}]\,p\}$$
$$+ \tbinom{s}{3}\{\alpha\gamma x^2z + dkxyz + \delta kx^2z + \beta kx^2y + 2\beta\gamma k\tbinom{x}{2}xz\}\,p$$
$$+ \beta yk\tbinom{s}{4}x^3zp + \tfrac{1}{2}\{\tfrac{1}{3!}s(s-1)(2s-1)z^2 - \tbinom{s}{2}z\}\{e\gamma x + d\gamma k\tbinom{x}{2}\}\,p$$
$$+ \tfrac{1}{2}d\gamma k\,[\tfrac{1}{2}(s-1)z^2 - z]\tbinom{s}{3}x^2.$$

A comparison of the generational equations of the present section with those of Sections 1 and 2, shows that, $\gamma \equiv 0 \pmod p$ gives groups simply isomorphic with those of Section 1, while $\beta \equiv 0 \pmod p$, groups simply

isomorphic with those of Section 2 and we need consider only the groups in which β and γ are prime to p.

5. *Transformation of the groups.* All groups of this section are given by equations (24), (25), and (26), where $\gamma,\ \beta = 1,\ 2, \cdots,\ p-1$; $\alpha,\ \delta,\ d,\ e = 0,\ 1,\ 2, \cdots, p-1$; and $\epsilon = 0,\ 1,\ 2,\ \cdots, p^2-1$. Not all of these, however are distinct. Suppose that G is simply isomorphic with G' and that the correspondence is given by

$$C = \begin{bmatrix} R, & Q, & P \\ R_1', & Q_1', & P_1' \end{bmatrix}.$$

An inspection of (30) gives

$$R_1' = Q'^{z''p} R'^{y''} P'^{x''p^{m-4}},$$

$$Q_1' = Q'^{z'} R'^{y'} P'^{x'p^{m-5}},$$

$$P_1' = Q'^{z} R'^{y} P'^{x},$$

with $dv\,[x,\ p] = 1$. Since Q^p is not in $\{P\}$, and R is not in $\{Q^p, P\}$, $Q_1'^p$ is not in $\{P_1'\}$ and R_1' is not in $\{Q_1'^p, P_1'\}$. Let

$$Q_1'^{s'p} = P_1'^{sp^{m-4}}.$$

This is in terms of R', Q', and P',

$$[0,\ s'z'p,\ s'x'p^{m-4}] = [0,\ 0,\ sxp^{m-4}].$$

From which

$$s'z'p \equiv 0 \pmod{p^2},$$

and z' must be prime to p, since otherwise s' can $= 1$. Let

$$R_1'^{s''} = Q_1'^{s'p} P_1'^{sp^{m-4}},$$

or in terms of R', Q', and P',

$$[s''y'',\ s''z''p,\ s''x''p^{m-4}] = [0,\ s'z'p,\ (sx + s'x')p^{m-4}]$$

and

$$s''z'' \equiv s'z' \pmod{p}, \qquad s''y'' \equiv 0 \pmod{p},$$

and y'' is prime to p, since otherwise s'' can $= 1$. Since R, Q, and P satisfy equations (24), (25) and (26), R_1', Q_1', and P_1' must also satisfy them. These become when reduced in terms of R', Q' and P'

$$[0,\ z + \theta_1' p,\ 0,\ y + \gamma' x z',\ 0,\ x + \psi_1' p^{m-5}]$$
$$= [0,\ z + \theta_1 p,\ 0,\ y + \gamma y'',\ 0,\ x + \psi_1 p^{m-5}],$$

$$[0, (z'' + \theta_2')p, 0, y'', 0, (x'' + \psi_2)p^{m-4}]$$
$$= [0, (z'' + \theta_2)p, 0, y'', 0, (x'' + \psi_2)p^{m-4}],$$
$$[0, z + \theta_3' p, 0, y, 0, x + \psi_3' p^{m-4}]$$
$$= [0, z + \theta_3 p, 0, y, 0, x + \psi_3 p^{m-4}],$$

where

$$\theta_1' = d'(yz' - y'z) + x\{d'\gamma'\tbinom{z'}{2} + \delta' z' + \beta' y'\} + \beta'\gamma'\tbinom{x}{2}z',$$
$$\theta_1 = \gamma z'' + \delta z' + d'\gamma y'' z,$$
$$\psi_1' = \epsilon' x z' + \{e'\gamma' x\tbinom{z'}{2} + \tbinom{x}{2}[\alpha'\gamma' z' + \gamma'\epsilon' d' k'\tbinom{z'}{2} + \delta'\epsilon k' z' + \beta' k' y']$$
$$+ \beta'\gamma'\tbinom{x}{3}z' + e'(yz' - y'z) + \alpha' x y'\}p,$$
$$\psi_1 = \epsilon x + \{\delta x' + \gamma x'' + e'\gamma y'' z\}p,$$
$$\theta_2' = d'y''z', \qquad \theta_2 = dz', \qquad \psi_2' = e'y''z', \qquad \psi_2 = dx' + ex,$$
$$\theta_3' = \beta' x y'' - d'y''z, \qquad \theta_3 = \beta z',$$
$$\psi_3 = \epsilon' x z'' - e'y''z + \alpha' x y'' + \beta'\epsilon\tbinom{x}{2}y'', \qquad \psi_3 = \alpha x + \beta x'.$$

A comparison of the two sides of these equations give seven congruences

(I) $$\theta_1' \equiv \theta_1 \pmod{p},$$

(II) $$\gamma' x z' \equiv \gamma y'' \pmod{p},$$

(III) $$\psi_1' \equiv \psi_1 \pmod{p^2},$$

(IV) $$\theta_2' \equiv \theta_2 \pmod{p},$$

(V) $$\psi_2' \equiv \psi_2 \pmod{p},$$

(VI) $$\theta_3' \equiv \theta_3 \pmod{p},$$

(VII) $$\psi_3' \equiv \psi_3 \pmod{p}.$$

(VI) is linear in z provided $d' \not\equiv 0 \pmod{p}$ and z may be so determined that $\beta \equiv 0 \pmod{p}$ and therefore all groups in which $d' \not\equiv 0 \pmod{p}$ are simply isomorphic with groups in Section 2.

Consequently we need only consider groups in which $d \equiv 0 \pmod{p}$.

As before we take for G' the simplest case and associate with it all simply isomorphic groups G. We then take as G' the simplest case left and proceed as above.

Let $\kappa = \kappa_1 p^{\kappa_2}$ where $dv[\kappa_1, p] = 1$, $(\kappa = \alpha, \beta, \gamma, \delta, \epsilon, d, e)$.

For convenience the groups are divided into three sets and each set is subdivided into eight cases.

The sets are given by

$$A: \quad \epsilon_2 = 0, \quad \beta_2 = 0, \quad \gamma_2 = 0,$$

$$B: \quad \epsilon_2 = 1, \quad \beta_2 = 0, \quad \gamma_2 = 0,$$

$$C: \quad \epsilon_2 = 2, \quad \beta_2 = 0, \quad \gamma_2 = 0.$$

The subdivision into cases and results of the discussion are given in Table I.

I.

	δ_2	ϵ_2	α_2	A	B	C
1	1	1	1			B_1
2	0	1	1	A_1	B_1	B_1
3	1	0	1			B_3
4	1	1	0	A_1	B_1	B_1
5	0	0	1	A_3	B_3	B_3
6	0	1	0	A_1	B_1	B_1
7	1	0	0	A_3	B_3	B_3
8	0	0	0	A_3	B_3	B_3

6. *Reduction to types.* The types of this section are given by equations (24), (25) and (26) with $\alpha = 0$, $\beta = 1$, $\lambda = 1$ or a quadratic non-residue $(\text{mod } p)$, $\delta \equiv 0$; $\epsilon = 1$, $e = 0, 1, 2, \cdots, p-1$; and $\epsilon = p$, $e = 0, 1$, or a non-residue $(\text{mod } p)$, $2p + 6$ in all.

The special forms of the congruences for these cases are given below.

A_1.

$$\text{(I)} \qquad \beta'\gamma'\tbinom{z}{2}z' + \beta'xy' \equiv \gamma z'' + \delta z' \pmod{p},$$

$$\text{(II)} \qquad \gamma'xz' \equiv \gamma y'' \pmod{p},$$

(III) $$\epsilon' x z' \equiv \epsilon x \pmod{p},$$

(IV) $$d z' \equiv 0 \pmod{p},$$

(V) $$e x \equiv 0 \pmod{p},$$

(VI) $$\beta' x y'' \equiv \beta z' \pmod{p},$$

(VII) $$\epsilon' x z'' + \beta' \epsilon' \binom{x}{2} y' \equiv \alpha x + \beta x' \pmod{p}.$$

(I) is linear in z'' and $\delta \equiv 0$ or $\not\equiv 0$, (II) gives $\gamma \not\equiv 0$, (III) $\epsilon \not\equiv 0$, (IV) and (V) $d \equiv e \equiv 0$, (VI) $\beta \not\equiv 0$, (VII) is linear in x' and $\alpha \equiv 0$ or $\not\equiv 0 \pmod{p}$.

Elimination of y'' and z' between (II) and (VI) gives

$$\beta' \gamma' x^2 \equiv \beta\gamma \pmod{p}$$

and $\beta\gamma$ is a residue or non-residue $(\bmod p)$ according as $\beta'\gamma'$ is a residue or non-residue.

A_3.

(I) $$\beta' \gamma' \binom{x}{2} z' + \beta' x y' \equiv \gamma z'' + \delta z' \pmod{p},$$

(II) $$\gamma' x z' \equiv \gamma y'' \pmod{p},$$

(III) $$\epsilon' z' \equiv \epsilon \pmod{p},$$

(IV) $$d \equiv 0 \pmod{p},$$

(V) $$e' y'' z' \equiv e x \pmod{p},$$

(VI) $$\beta' x y'' \equiv \beta z' \pmod{p},$$

(VII) $$\epsilon' x z'' - e' y'' z + \beta' \epsilon' \binom{x}{2} y' \equiv \alpha x + \beta x' \pmod{p}.$$

(I) is linear in z'' and $\delta \equiv 0$ or $\not\equiv 0$. (II) gives $\gamma \not\equiv 0$, (III) $\epsilon \not\equiv 0$, (V) $e \not\equiv 0$ and (VI) $\beta \not\equiv 0$. (VII) is linear in x' and $\alpha \equiv 0$ or $\not\equiv 0 \pmod{p}$.

Elimination between (II) and (VI) gives

$$\beta' \gamma' x^2 \equiv \beta\gamma \pmod{p},$$

and between (II), (III), and (IV) gives

$$\epsilon'^2 \gamma e \equiv \epsilon^2 \gamma' e' \pmod{p}.$$

$\beta\gamma$ is a residue, or non-residue, according as $\beta'\gamma'$ is or is not, and if γ and ϵ are fixed, e must take the $(p-1)$ values $1, 2, \cdots, p-1$.

B$_1$.

(I) $$\beta'\gamma'\binom{z}{2}z' + \beta' xy' \equiv \gamma z'' + \delta z' \pmod{p},$$

(II) $$\gamma' xz' \equiv \gamma y'' \pmod{p},$$

(III) $$\epsilon_1' xz' + \beta' xz'\binom{z}{3} \equiv \epsilon_1 x + \delta x' + \gamma x'' \pmod{p},$$

(IV) $$ex \equiv 0 \pmod{p},$$

(VI) $$\beta' xy'' \equiv \beta z' \pmod{p},$$

(VII) $$\alpha x + \beta x' \equiv 0 \pmod{p}.$$

(I) gives $\delta \equiv 0$ or $\not\equiv 0$, (II) $\gamma \not\equiv 0$, (III) is linear in x'' and gives $\epsilon_1 \equiv 0$ or $\not\equiv 0$, (V) $e \equiv 0$, (VI) $\beta \not\equiv 0$ and (VII) is linear in x' and gives $\alpha \equiv 0$ or $\not\equiv 0$.

Elimination between (II) and (VI) gives

$$\beta'\gamma' x^2 \equiv \beta\gamma \pmod{p}.$$

B$_3$.

(I) $$\beta'\gamma'\binom{z}{2}z' + \beta' xy' \equiv \gamma\beta'' + \delta z' \pmod{p},$$

(II) $$\gamma' xz' \equiv \gamma y' \pmod{p},$$

(III) $$\epsilon_1' xz' + e'\gamma' x\binom{z'}{2} + \beta'\gamma'\binom{z}{3} + e'(yz' - y'z)$$
$$\equiv \epsilon_1 x + \delta x' + \gamma x'' + e'\gamma z y'' \pmod{p},$$

(V) $$e' y'' z' \equiv ex \pmod{p}.$$

(VI) $$\beta' xy'' \equiv \beta z' \pmod{p},$$

(VII) $$-e' y'' z \equiv \alpha x + \beta x' \pmod{p},$$

(I) gives $\delta \equiv 0$ or $\not\equiv 0$, (II) $\gamma \not\equiv 0$, (III) is linear in x'' and gives $\epsilon_1 \equiv 0$ or $\not\equiv 0$, (V) $e \not\equiv 0$, (VI) $\beta \not\equiv 0$, (VII) is linear in x' and gives $\alpha \equiv 0$ or $\not\equiv 0$ $\pmod{p}$. Elimination of y'' and z' between (II) and (VI) gives

$$\beta'\gamma' x^2 \equiv \beta\gamma \pmod{p},$$

and between (V) and (VI) gives

$$\beta' e' y''^2 \equiv \beta e \pmod{p}$$

and $\beta\gamma$ and βe are residues or non-residues, independently, according as $\beta'\gamma'$ and $\beta' e'$ are residues or non-residues.

Class III.

1. *General relations.* In this class, the pth power of every operator of G is contained in $\{P\}$. There is in G a subgroup H_1 of order p^{m-2}, which contains $\{P\}$ self-conjugately.*

2. *Determination of H_1.* H_1 is generated by P and some operator Q_1 of G.

$$Q_1^p = P^{hp}.$$

Denoting $Q_1^a P^b Q_1^c P^d \cdots$ by the symbol $[a, b, c, d, \cdots]$, all operators of H_1 are included in the set $[y, x]$; $(y = 0, 1, 2, \cdots, p-1, x = 0, 1, 2, \cdots, p^{m-3}-1)$.

Since $\{P\}$ is self-conjugate in H_1

(1) $$Q_1^{-1} P Q_1 = P^{1+kp^{m-4}}.\dagger$$

Hence

(2) $$[-y, x, y] = [0, x(1+kyp^{m-4})] \qquad (m>4).$$

and

(3) $$[y, x]^s = [sy, x\{s + ky\tbinom{s}{2}p^{m-4}\}].$$

Placing $y = 1$ and $s = p$ in (3), we have,

$$[Q_1 P^x]^p = Q_1^p P^{xp} = P^{(x+h)p}$$

and if x be so chosen that

$$(x+h) \equiv 0 \pmod{p^{m-4}},$$

$Q = Q_1 P^x$ will be an operator of order p which will be used in place of Q_1, $Q^p = 1$.

3. *Determination of H_2.* There is in G a subgroup H_2 of order p^{m-1}, which contains H_1 self-conjugately. H_2 is generated by H_1, and some operator R_1 of G.

$$R_1^p = P^{lp}.$$

We will now use the symbol $[a, b, c, d, e, f, \cdots]$ to denote $R_1^a Q^b P^c R_1^d Q^e P^f \cdots$.

The operations of H_2 are given by $[z, y, x]$; $(z, y = 0, 1, \cdots, p-1; x = 0, 1, \cdots, p^{m-3}-1)$. Since H_1 is self-conjugate in H_2

(4) $$R_1^{-1} P R_1 = Q_1^{\beta} P^{a_1},$$

(5) $$R_1^{-1} Q R_1 = Q_1^{b_1} P^{ap^{m-4}}.$$

---

* BURNSIDE, *Theory of Groups*, Art. 54, p. 64.

† Ibid., Art. 56, p. 66.

From (4), (5) and (3)

$$[-p, 0, 1, p] = \left[0, \frac{\alpha_1^p - b_1^p}{\alpha_1 - b_1}\beta, \alpha_1^p + \theta p^{m-4}\right] = [0, 0, 1],$$

where

$$\theta = \frac{\alpha_1^p \beta k}{2} \frac{\alpha_1^p - 1}{\alpha_1 - 1} + a\beta\left\{\frac{\alpha_1^p - 1}{\alpha_1 - b_1}p - \frac{\alpha_1^p - b_1^p}{(\alpha_1 - b_1)^2}\right\}.$$

Hence

(6) $$\frac{\alpha_1^p - b_1^p}{\alpha_1 - b_1}\beta \equiv 0 \pmod p, \qquad \alpha_1^p + \theta p^{m-4} \equiv 1 \pmod{p^{m-3}},$$

and $\alpha_1^p \equiv 1 \pmod{p^{m-4}}$, or $\alpha_1 \equiv 1 \pmod{p^{m-5}}$ $(m > 5)$, $\alpha_1 = 1 + \alpha_2 p^{m-5}$.
Equation (4) is replaced by

(7) $$R_1^{-1} P R_1 = Q^\beta P^{1+\alpha_2 p^{m-5}},$$

From (5), (7) and (3)

$$[-p, 1, 0, p] = \left[0, b_1^p, a\frac{b_1^p - 1}{b - 1}p^{m-4}\right].$$

Placing $x = lp$ and $y = 1$ in (2) we have $Q^{-1}P^{lp}Q = P^{lp}$, and

$$b_1^p \equiv 1 \pmod p, \qquad a\frac{b_1^p - 1}{b_1 - 1} \equiv 0 \pmod p.$$

Therefore, $b_1 = 1$.

Substituting 1 for b_1 and $1 + \alpha_2 p^{m-5}$ for α_1 in congruence (6) we find

$$(1 + \alpha_2 p^{m-5})^p \equiv 1 \pmod{p^{m-3}}, \qquad \text{or} \qquad \alpha_2 \equiv 0 \pmod p.$$

Let $\alpha_2 = \alpha p$ and equations (7) and (5) are replaced by

(8) $$R_1^{-1} P R_1 = Q^\beta P^{1+\alpha p^{m-4}},$$

(9) $$R_1^{-1} Q R_1 = Q P^{ap^{m-4}}.$$

From (8), (9) and (3)

(10) $$[-y, 0, x, y] = [0, \beta xy, x + \{\alpha xy + a\beta x\tbinom{y}{2} + \beta k y\tbinom{x}{2}\}p^{m-4}],$$

(11) $$[-y, x, 0, y] = [0, x, axyp^{m-4}].$$

From (2), (10), and (11)

(12) $$[z, y, x]^s = [sz, sy + U_s, sx + V_s p^{m-4}],$$

where

$$U_s = \beta\binom{s}{2}xz,$$

$$V_s = \binom{s}{2}\{axz + kxy + ayz + \beta k\binom{z}{2}z\} + \beta k\binom{s}{3}x^2z + \tfrac{1}{2}a\beta\binom{s}{2}\{\tfrac{1}{3!}(2s-1)z-1\}xz.$$

Placing $z=1$, $y=0$, and $s=p$ in (12)

$$[R_1P^x]^p = R_1^pP^{xp} = P^{(x+l)p}.*$$

If x be so chosen that

$$x + l \equiv 0 \pmod{p^{m-4}}$$

then $R = R_1P^x$ is an operator of order p which will be used in place of R_1 and $R^p = 1$.

4. *Determination of* G. G is generated by H_2 and some operation S_1.

$$S_1^p = P^{\lambda p}.$$

Denoting $S_1^aR^bQ^cP^d\cdots$ by the symbol $[a, b, c, d, \cdots]$ all the operators of G are given by

$$[v, z, y, x];\ (v, z, y = 0, 1, \cdots, p-1;\ x = 0, 1, \cdots, p^{m-3}-1).$$

Since H_2 is self-conjugate in G

(13) $$S_1^{-1}PS_1 = R^\gamma Q^\delta P^{\epsilon_1},$$

(14) $$S_1^{-1}QS_1 = R^cQ^dP^{ep^{m-4}},$$

(15) $$S_1RS_1 = R^fQ^gP^{jp^{m-4}}.$$

From (13), (14), (15), and (12)

$$[-p, 0, 0, 1, p] = [0, L, M, \epsilon_1^p + Np^{m-4}] = [0, 0, 0, 1]$$

and

$$\epsilon_1^p \equiv 1 \pmod{p^{m-4}} \quad \text{or} \quad \epsilon_1 \equiv 1 \pmod{p^{m-5}} \qquad (m>5).$$

Let $\epsilon_1 = 1 + \epsilon_2p^{m-5}$. Equation (13) is now replaced by

(16) $$S_1^{-1}PS_1 = R^\gamma Q^\delta P^{1+\epsilon_2p^{m-5}}.$$

$$\text{If } \lambda \equiv 0 \pmod{p} \qquad \text{and} \qquad \lambda = \lambda' p,$$

* The terms of the form $(Ax+Bx^2)p^{m-4}$ which appear in the exponent of P for $p=3$ do not alter the conclusion for $m>5$.

$$[1, 0, 0, 1]^p = [p, 0, 0, p + \epsilon \tbinom{p}{2} p^{m-5} + Wp^{m-4}]$$
$$= [0, 0, 0, p + \lambda' p^2 + W' p^{m-4}]$$

and for $m > 5$ $S_1 P$ is of order p^{m-3}. We will take this in place of S_1 and assume $dv\,[\lambda, p] = 1$.

$$S_1^{p^{m-3}} = 1.$$

There is in G a subgroup H_1' of order p^{m-2} which contains $\{S_1\}$ self-conjugately. $H_1' = \{S_1, S_1^v R^z Q^y P^x\}$ and the operator $T = R^z Q^y P^x$ is in H_1'.

There are two cases for discussion.

1°. Where x is prime to p.

T is an operator of H_2 of order p^{m-3} and will be taken as P. Then

$$H_1' = \{S_1, P\}.$$

Equation (16) becomes

$$S_1^{-1} P S_1 = P^{1+\epsilon p^{m-4}}.$$

There is in G a subgroup H_2' of order p^{m-1} which contains H_1' self-conjugately.

$$H_2' = \{H_1', S_1^{v'} R^{z'} Q^{y'} P^{x'}\}.$$

$T' = R^{z'} Q^{y'}$ is in H_2' and also in H_2 and is taken as Q, since $\{P, T'\}$ is of order p^{m-2}.

$H_2' = \{H_1', Q\} = \{S_1, H_1\}$ and in this case c may be taken $\equiv 0 \pmod p$.

2°. *Where* $x = x_1 p$. P^p is in $\{S_1\}$ since λ is prime to p. In the present case $R^z Q^y$ is in H_1' and also in H_2. If $z \not\equiv 0 \pmod p$ take $R^z Q^y$ as R; if $z \equiv 0 \pmod p$ take it as Q.

$$H_1' = \{S_1, R\} \qquad \text{or} \qquad \{S_1, Q\},$$

and

$$R^{-1} S_1 R = S_1^{1+k' p^{m-4}} \qquad \text{or} \qquad Q^{-1} S_1 Q = S_1^{1+k'' p^{m-4}}.$$

On rearranging these take the forms

$$S_1^{-1} R S_1 = R S_1^{n p^{m-4}} = R P^{j p^{m-4}} \qquad \text{or} \qquad S_1^{-1} Q S_1 = Q S_1^{n' p^{m-4}} = Q P^{c p^{m-4}},$$

and either c or g may be taken $\equiv 0 \pmod p$,

(17) $$cg \equiv 0 \pmod p.$$

From (14), (15), (16), (12) and (17)

$$[-p, 0, 1, 0, p] = \left[0,\ c\frac{d^p - f^p}{d - f},\ d^p,\ Wp^{m-4}\right].$$

Place $x = \lambda p$ and $y = 1$ in (12)

$$Q^{-1}P^{\lambda p}Q = P^{\lambda p} \qquad \text{or} \qquad S_1^pQS_1^p = Q,$$

and

$$d^p \equiv 1 \pmod p, \qquad d = 1.$$

Equation (14) is replaced by

$$S_1^{-1}QS_1 = R^cQP^{ep^{m-4}}. \tag{18}$$

From (15), (18), (17), (16) and (12)

$$[-p, 1, 0, 0, p] = \left[0, f^p, \frac{d^p - f^p}{d - f}g, W'p^{m-4}\right].$$

Placing $x = \lambda p$, $y = 1$ in (10)

$$R^{-1}P^{\lambda p}R = P^{\lambda p},$$

and $f^p \equiv 1 \pmod p$, $f = 1$. Equation (15) is replaced by

$$S_1^{-1}RS_1 = RQ^gP^{jp^{m-4}}. \tag{19}$$

From (16), (18), (19) and (12)

$$S_1^{-p}PS_1^p = P^{1+\epsilon_2p^{m-4}} = P$$

and $\epsilon_2 \equiv 0 \pmod p$. Let $\epsilon_2 = \epsilon p$ and (16) is replaced by

$$S_1^{-1}PS_1 = R^\gamma Q^\delta P^{1+\epsilon p^{m-4}}. \tag{20}$$

Transforming both sides of (1), (8) and (9) by S_1

$$S_1^{-1}Q^{-1}S_1 \cdot S_1^{-1}PS_1 \cdot S_1^{-1}QS_1 = S_1^{-1}P^{1+kp^{m-4}}S_1,$$

$$S_1^{-1}R^{-1}S_1 \cdot S_1^{-1}PS_1 \cdot S_1^{-1}RS_1 = S_1^{-1}Q^\beta S_1 \cdot S_1^{-1}P^{1+ap^{m-4}}S_1,$$

$$S_1^{-1}R^{-1}S_1 \cdot S_1^{-1}QS_1 \cdot S_1^{-1}RS_1 = S_1^{-1}QS_1 \cdot S_1^{-1}P^{ap^{m-4}}S_1.$$

Reducing these by (18), (19), (20) and (12) and rearranging

$$[0, \gamma, \delta + \beta c, 1 + \{\epsilon + ac + k + ac\delta + a\beta\tbinom{c}{2} - a\gamma\}p^{m-4}]$$
$$= [0, \gamma, \delta, 1 + (\epsilon + k)p^{m-4}].$$

$$[0, \gamma, \beta + \delta, 1 + \{kg + \epsilon + a + a\delta - a\gamma g\}p^{m-4}]$$
$$= [0, \gamma + \beta c, \beta + \delta, 1 + \{\epsilon + a + \beta e + a\tbinom{\beta}{2}c + a\beta\gamma\}p^{m-4}],$$

$$[0, c, 1, (e + a)p^{m-4}] = [0, c, 1, (e + a)p^{m-4}].$$

The first gives

(21) $$\beta c \equiv 0 \pmod{p},$$

(22) $$ac + ac\delta - a\gamma \equiv 0 \pmod{p}.$$

Multiplying this last by g

(23) $$ag\gamma \equiv 0 \pmod{p}.$$

From the second equation above

(24) $$gk + a\delta \equiv \beta e + a\beta\gamma \pmod{p}.$$

Multiplying by c

(25) $$ac\delta \equiv 0 \pmod{p}.$$

These relations among the constants *must be satisfied* in order that our equations should define a group.

From (20), (19), (18) and (12)

(26) $$[-y, 0, 0, x, y] = [0, \gamma xy + \chi_1(x, y), \delta xy + \phi_1(x, y), x + \Theta_1(x, y)p^{m-4}],$$

(27) $$[-y, 0, x, 0, y] = [0, cxy, x, \Theta_2(x, y)p^{m-4}],$$

(28) $$[-y, x, 0, 0, y] = [0, x, gxy, \Theta_3(x, y)p^{m-4}],$$

where

$$\chi_1(x, y) = c\delta x\tbinom{y}{2},$$

$$\phi_1(x, y) = \gamma gx\tbinom{y}{2} + \beta\gamma\tbinom{x}{2}y,$$

$$\Theta_1(x, y) = exy + \tbinom{y}{2}[\gamma jx + e\delta x + a\delta\gamma + (a\gamma + k\delta)\tbinom{x}{2}] + \tbinom{y}{3}[c\delta j + eg\gamma]x + \tbinom{x}{2}[a\gamma y + \delta ky + a\delta\gamma y^2] + \beta\gamma k\tbinom{x}{3}y,$$

$$\Theta_2(x, y) = exy + cjx\tbinom{y}{2} + ac\tbinom{x}{2}y,$$

$$\Theta_3(x, y) = jxy + egx\tbinom{y}{2} + ag\tbinom{x}{2}y.$$

Let a general power of any operator be

(29) $$[v, z, y, x]^s = [sv, sz + U_s, sy + V_s, sx + W_s p^{m-4}].$$

Multiplying both sides by $[v, z, y, x]$ and reducing by (2), (10), (11), (26), (27) and (28), we find

$$U_{s+1} \equiv U_s + (cy + \gamma x)sv + c\delta\binom{sv}{2}x \pmod p,$$

$$V_{s+1} \equiv V_s + (gz + \delta x)sv + \gamma g\binom{sv}{2}x + \beta\gamma\binom{x}{2}sv + \beta(sz + U_s)x \pmod p,$$

$$\begin{aligned} W_{s+1} = W_s + \Theta_1(x, sv) + \{ & ey + jz + a\gamma xy + ac\binom{y}{2} \\ & + ag\binom{z}{2}\} sv + \{ax + \beta k\binom{x}{2} + ay + a\delta sx + agsvz\} sz \\ & + ksxy + \binom{sv}{2}\{cjy + egz\} + U_s\{ax + \beta k\binom{x}{2} + ay \\ & + a(\delta x + gz)sv\} + a\beta\binom{sz + U_s}{2}x + kV_s x \pmod p. \end{aligned}$$

From (29)

$$U_1 \equiv 0, \qquad V_1 \equiv 0, \qquad W_1 \equiv 0 \pmod p.$$

A continued use of the above congruences give

$$U_s \equiv (cy + \gamma x)\binom{s}{2}v + \tfrac{1}{2}c\delta xv\{\tfrac{1}{3}(2s - 1)v - 1\}\binom{s}{2} \pmod p,$$

$$\begin{aligned} V_s \equiv \{[gz + \delta x + \beta\gamma\binom{x}{2}v + \beta xz\}\binom{s}{2} + \tfrac{1}{2}\gamma gxv\{\tfrac{1}{3}(2s - 1)v - 1\}\binom{s}{2} \\ + \beta\gamma\binom{s}{3}x^2 v \pmod p, \end{aligned}$$

$$\begin{aligned} W_s \equiv \binom{s}{2}\{ & exv + egv + (a\gamma + \delta kv + \beta kz)\binom{x}{2} + \beta\gamma k\binom{x}{3}v + ac\binom{y}{2}v \\ & + jvz + ag\binom{z}{2}v + axz + kxy + a\gamma xyv + ayz\} + \binom{s}{3}\{acxyv \\ & + a\gamma x^2 v + 2\beta\gamma k\binom{x}{2}xv + gkxzv + \delta kx^2 v + \beta kx^2 z + acvy^2 \\ & + a\gamma xvy\} + \beta k\gamma\binom{s}{4}x^3 v + \binom{s}{2}\frac{2s - 1}{3}\{a\delta\gamma\binom{x}{2}v^2 + a\delta xzv \\ & + agvz^2\} + \tfrac{1}{2}v\binom{s}{2}\{\tfrac{1}{3}(2s - 1)v - 1\}\{\gamma jx + e\delta x + a\delta\gamma x \\ & + ac\delta\binom{x}{2} + \gamma gk\binom{x}{2} + cjy + egz\} + \tfrac{1}{6}\binom{s}{2}\{\binom{s}{2}v^2 - (2s - 1)v \\ & + 2\}\{c\delta jx + eg\gamma x\}v + \tfrac{1}{2}\binom{s}{3}\{\tfrac{1}{2}(s - 1)v - 1\}\{ac\delta \\ & + \gamma gk\}x^2 v + \tfrac{1}{2}a\beta x\binom{s}{2}\{\tfrac{1}{3}(2s - 1)z - 1\}z \\ & + \tfrac{1}{2}a\delta\gamma x^2 v\binom{s}{3}\tfrac{1}{2}(3s - 1) \pmod p. \end{aligned}$$

Placing $v = 1, z = y = s = p$ in (29)

$$[S_1 P^x]^p = S_1^p P^{xp} = P^{(\lambda+x)p} \qquad (p > 3)^*.$$

If x be so chosen that

$$x + \lambda \equiv 0 \pmod{p^{m-4}}.$$

$S = S_1 P^x$ is an operator of order p and is taken in place of S_1.

$$S^p = 1.$$

The substitution of S for S_1 leaves congruence (17) invariant.

5. *Transformation of the groups.* All groups of this class are given by

$$(30) \qquad G: \begin{cases} Q^{-1}PQ = P^{1+kp^{m-4}}, \\ R^{-1}PR = Q^{\beta} P^{1+ap^{m-4}}, \\ R^{-1}QR = QP^{ap^{m-4}}, \\ S^{-1}PS = R^{\gamma} Q^{\delta} P^{1+\epsilon p^{m-4}}, \\ S^{-1}QS = R^{c} QP^{ep^{m-4}}, \\ S^{-1}RS = RQ^{g} P^{jp^{m-4}}, \end{cases}$$

with

$$P^{p^{m-3}} = 1, \qquad Q^p = R^p = S^p = 1,$$

$(k, \beta, \alpha, a, \gamma, \delta, \epsilon, c, e, g, j = 0, 1, 2, \cdots, p-1)$.

These constants are however subject to conditions (17), (21), (22), (23), (24) and (25). Not all these groups are distinct. Suppose that G and G' of the above set are simply isomorphic and that the correspondence is given by

$$C = \begin{bmatrix} S, & R, & Q, & P \\ S_1', & R_1', & Q_1', & P_1' \end{bmatrix}.$$

Inspection of (29) gives

$$S_1' = S'^{v'''} R'^{z'''} Q'^{y'''} P'^{x'''p^{m-4}},$$

$$R_1' = S'^{v''} R'^{z''} Q'^{y''} P'^{x''p^{m-4}},$$

$$Q_1' = S'^{v'} R'^{z'} Q'^{y'} P'^{x'p^{m-4}},$$

$$P_1' = S'^{v} R'^{z} Q'^{y} P'^{x},$$

---

* For $p = 3$ and $c\delta \equiv \gamma g \equiv \beta\gamma \equiv 0 \pmod{p}$ there are terms of the form $(A + Bx + Cx^2 + Dx^3)p^{m-4}$ in the exponent of P. For $m > 5$ these do not vitiate our conclusion. For $p = 3$ and $c\delta$, γg, or $\beta\gamma$ prime to p, $[S_1 P^x]^p$ is not contained in $\{P\}$ and the groups defined belong to Class II.

in which x and one out of each of the sets v', z', y', x'; v'', z'', y'', x''; v''', z''', y''', x'''; are prime to p.

Since S, R, Q, and P satisfy equations (30), S_1', R_1', Q_1', and P_1' also satisfy them. Substituting these operators and reducing in terms of S', R', Q', and P' we get the six equations

$$(31) \qquad [V_\kappa', Z_\kappa', Y_\kappa', X_\kappa'] = [V_\kappa, Z_\kappa, Y_\kappa, X_\kappa] \quad (\kappa = 1, 2, 3, 4, 5, 6),$$

which give the following twenty-four congruences

$$(32) \qquad \begin{cases} V_\kappa' \equiv V_\kappa \pmod{p}, \\ Z_\kappa' \equiv Z_\kappa \pmod{p}, \\ Y_\kappa' \equiv Y_\kappa \pmod{p}, \\ X_\kappa' \equiv X_\kappa \pmod{p^{m-3}}, \end{cases}$$

where

$$V_1' = v, \qquad V_1 = v,$$

$$Z_1' = z + c'(yv' - y'v) + \gamma' xv' + c\delta x\binom{v'}{2}, \qquad Z_1 = z,$$

$$Y_1' = y + g'(zv' - z'v) + \delta' xv' + \gamma' g' x\binom{v}{2} + \beta' xz', \qquad Y_1 = y,$$

$$\begin{aligned} X_1' = x + \{&\epsilon' xv' + (\gamma' j'' x + e'\delta' x + a'\delta'\gamma' x)\binom{v'}{2} + c'\delta' j''\binom{v'}{3} + (\alpha'\gamma' v' + \delta' k' v' \\ &+ a'\delta'\gamma' v^2 + \beta' k' z')\binom{x}{2} + j''(zv' - z'v) + e'g'[z\binom{v'}{2} - z'\binom{v}{2}] \\ &+ a'g'[\binom{z}{2}v' + \binom{z'}{2i}v - zz'v] + e'(yv' - y'v) + c'j''[y\binom{v'}{2} - y'\binom{v}{2}] \\ &+ a'c'[\binom{y}{2}v' + v\binom{-y'}{2} - yy'v] + a'(yz' - y'z) - a'\beta' xz'^2 + \alpha' xz' \\ &+ \alpha'\beta' x\binom{z'}{2} + a'\gamma' x(y - y')v' + k' xy'\} p^{m-4}, \end{aligned}$$

$$X_1 = x + kxp^{m-4},$$

$$V_2' = v, \qquad V_2 = v + \beta v',$$

$$Z_2' = z + c'(yv'' - y''v) + \gamma' xv'' + e'\delta'\binom{v''}{2}, \qquad Z_2 = z + \beta z' + c'\beta y'v,$$

$$Y_2' = y + g'(zv'' - z''v) + \delta' xv'' + \gamma' g' x\binom{v''}{2} + \beta'\gamma'\binom{x}{2}v'' + \beta' xz'',$$

$$Y_2 = y + \beta y' + g'\beta z'v,$$

$$X'_2 = x + \{\Theta'_1(x,\, v'') + j'(zv'' - z''v) + e'g'[z\tbinom{v''}{2} - z''\tbinom{v}{2}] + a'g'[\tbinom{z}{2}v''$$

$$+ \tbinom{-z''}{2}v - zz''v] + e'(yv'' - y''v) + c'j'[y\tbinom{v''}{2} - y''\tbinom{v}{2}] + a'c'[\tbinom{y}{2}v''$$

$$+ \tbinom{-y''}{2}v - yy''v''] + a'g'(zv'' - z''v)z'' + a'(yz'' - y''z) + a'\delta'v''z''$$

$$+ a'\gamma'(y - y'')v''x + \alpha'xz'' + a'\beta'x\tbinom{z''}{2} + \beta'k'\tbinom{x}{2}z'' + k'xy''\}\,p^{m-4},$$

$$X_2 = x + \{\alpha x + \beta x' + a'\tbinom{\beta}{2}y'z' + e'\beta vy' + (c'j'\beta + e'g'\beta z')\tbinom{v}{2}$$

$$+ a'c'\tbinom{\beta y'}{2}v + j'\beta vz' + a'g'\tbinom{\beta z'}{2} + a'\beta(g'z'v + y')z\}\,p^{m-4},$$

$$V'_3 = v', \qquad V_3 = v',$$

$$Z'_3 = z' + c'(y'v'' - y''v'), \qquad Z_3 = z',$$

$$Y'_3 = y' + g'(z'v'' - z''v'), \qquad Y_3 = y',$$

$$X'_3 = \{x' + j'(z'v'' - z''v') + e'g'[\tbinom{v''}{2}z' - \tbinom{v'}{2}z''] + a'g'[\tbinom{z'}{2}v'' + \tbinom{-z''}{2}v'$$

$$- z'z''v'] + e'(y'v'' - y''v') + c'j'[y'\tbinom{v''}{2} - y''\tbinom{v'}{2}] + a'c'[\tbinom{y'}{2}v'' + \tbinom{-y''}{2}v'$$

$$- y''y'v''] + a'(y'z'' - y''z')\}\,p^{m-4},$$

$$X_4 = (x' + a'x)\,p^{m-4},$$

$$V'_4 = v, \qquad V_4 = v + \gamma v'' + \delta v',$$

$$Z'_4 = z + c'(yv''' - y'''v) + \gamma'xv''' + c'\delta'x\tbinom{v'''}{2},$$

$$Z_4 = z + \gamma z'' + \delta z' + c'[\tbinom{\gamma}{2}v''y'' + \tbinom{\delta}{2}v'y' + c'(\gamma y'' + \delta y')v + c'\gamma\delta y''v,$$

$$Y'_4 = y + g'(zv''' - z'''v) + \delta'xv''' + \gamma'g'x\tbinom{v'''}{2} + \beta'\gamma'\tbinom{x}{2}v''' + \beta'xz''',$$

$$Y_4 = y + \gamma y'' + \delta y' + g'[\tbinom{\gamma}{2}v''z'' + \tbinom{\delta}{2}v'z'] + g'(\gamma z'' + \delta z')v + g'\delta\gamma v'z'',$$

$$X'_4 = x + \{\Theta'_1(x,\, v''') + j'(zv''' - z'''v) + e'g'[\tbinom{v'''}{2}z - \tbinom{v}{2}z'''] + a'g'[\tbinom{z}{2}v'''$$

$$+ \tbinom{-z'''}{2}v - zz'''v] + e'(yv''' - y'''v) + c'j'[y\tbinom{v'''}{2} - y'''\tbinom{v}{2}]$$

$$+ a'c'[\tbinom{y}{2}v''' + \tbinom{-y'''}{2}v - yy'''v'''] + a'g'(v'''z - vz''')z'''$$

$$+ a'(yz''' - y'''z) + a'\delta'xz'''v''' + a'\gamma'x(y - y''')v''' + \alpha'xz'''$$

$$+ a'\beta'x\tbinom{z'''}{2} + \beta'k'z'''\tbinom{x}{2} + k'xy'''\}\,p^{m-4}.$$

$$
\begin{aligned}
X_4 = x + \{ & \epsilon x + \delta x' + \gamma x'' + \tbinom{\gamma}{2}\big[a'c'\tbinom{y''}{2}v'' + a'y''z'' + e'v''y'' + j'v''z'' \\
& + a'g'\tbinom{z''}{2}v'' + (c'j'v''y'' + e'g'v''z'')(v + \delta v') + a'(z + \delta z')v''z'' \\
& + \frac{2\gamma - 1}{3}a'g'v''z''^2 + \tfrac{1}{2}\big[\tfrac{1}{3}(2\gamma - 1)v'' - 1\big](c'j'y'' + e'g'z'')v''\big] \\
& + \tbinom{\gamma}{3}a'c'v''y'' + \tbinom{\delta}{2}\big[a'c'\tbinom{y'}{2}v' + a'y'z' + e'v'y' + j'v'z' \\
& + a'g'\tbinom{z'}{2}v' + j'c'vv'y' + e'g'vv'z' + a'g'v'zz' + a'c'\gamma y'y''v' \\
& + \frac{2\delta - 1}{3}a'g'v'z'^2 + \tfrac{1}{2}\{\tfrac{1}{3}(2\delta - 1)v' - 1\}(c'j'y' + e'g'z')\big] \\
& + \tbinom{\delta}{3}a'c'v'y'^2 + (v + \delta v')\big[j'\gamma z'' + \tbinom{\gamma z''}{2}a'g' + e'\gamma y'' + \tbinom{\gamma y''}{2}a'c' \\
& + a'g'(z + \delta z')\big] + \tbinom{v + \delta v'}{2}\big[e'g'\gamma z'' + c'j'\gamma y''\big] + \delta\big[(e'g'z' \\
& + c'j'y')\tbinom{v}{2} + e'vy' + j'z' + a'zy + a'g'vzz' + a'\gamma z'y'' + a'c'\gamma vy'y''\big] \\
& + a'g'\tbinom{\delta z'}{2}v + a'c'\tbinom{\delta y'}{2}v + a'\gamma zy''\}\, p^{m-4},
\end{aligned}
$$

$$V_5' = v', \qquad V_5 = v' + cv'',$$

$$Z_5' = z' + c'(y'v''' - y'''v'), \qquad Z_5 = z' + cz'' + c'cy''v,$$

$$Y_5' = y' + g'(z'v''' - z'''v'), \qquad Y_5 = y' + cy'' + g'cv'z'',$$

$$
\begin{aligned}
X_5' = \{ & x' + j'(z'v''' - z'''v') + e'g'\big[\tbinom{v'''}{2}z' - \tbinom{v'}{2}z'''\big] + a'g'\big[\tbinom{z'}{2}v''' \\
& + \tbinom{-z'''}{2}v' - z'z'''v'\big] + e'(y'v''' - y'''v') + c'j'\big[y'\tbinom{v'''}{2} - y'''\tbinom{v'}{2}\big] \\
& + a'c'\big[\tbinom{y'}{2}v''' + \tbinom{-y'''}{2}v' - y'y'''v'''\big] + a'(y'z''' - y'''z')\}\, p^{m-4},
\end{aligned}
$$

$$
\begin{aligned}
X_5 = \{ & x' + ex + cx'' + a'\tbinom{c}{2}y''z'' + j'cv'z'' + (e'g'cz'' + c'cj'y'')\tbinom{v'}{2} + e'cy''v \\
& + a'cy''z' + a'g'z'v' + a'g'\tbinom{cz''}{2} + a'c'\tbinom{cy''}{2},
\end{aligned}
$$

$$V_6' = v'', \qquad V_6 = v'' + gv',$$

$$Z_6' = z'' + c'(y''v''' - y'''v''), \qquad Z_6 = z'' + gz',$$

$$Y_6' = y'' + g'(z''v''' - z'''v''), \qquad Y_6 = y'' + gy',$$

$$
\begin{aligned}
X_6' = \{ & x'' + j'(z''v''' - z'''v'') + e'g'\big[\tbinom{v'''}{2}z'' - \tbinom{v''}{2}z'''\big] + a'g'\big[\tbinom{z''}{2}v''' \\
& + \tbinom{-z'''}{2}v'' - z''z'''v''\big] + e'(y''v''' - y'''v'') + c'j'\big[y''\tbinom{v'''}{2} - y'''\tbinom{v''}{2}\big] \\
& + a'c'\big[\tbinom{y''}{2}v''' + \tbinom{-y'''}{2}v'' - y''y'''v'''\big] + a'(y''z''' - y'''z'')\}\, p^{m-4},
\end{aligned}
$$

$$X_6 = \{x'' + jx + gx' + a'gy''z'\}\, p^{m-4}.$$

The necessary and sufficient condition for the simple ismorphism of the two groups G and G' is *that congruences* (32) *shall be consistent and admit of solution* subject to conditions derived below.

6. *Conditions of transformation.* Since Q is not contained in $\{P\}$, R is not contained in $\{Q, P\}$, and S is not contained in $\{R, Q, P\}$, then Q_1' is not contained in $\{P_1'\}$, R_1' is not contained in $\{Q_1', P_1'\}$, and S_1' is not contained in $\{R_1', Q_1', P_1'\}$.

Let

$$Q_1'^{s'} = P_1'^{xp^{m-4}}.$$

This equation becomes in terms of S', R', Q' and P'

$$[s'v', s'z' + c'\tbinom{s'}{2}v'y', s'y' + g'\tbinom{s'}{2}v'z', Dp^{m-4}] = [0, 0, 0, sxp^{m-4}],$$

and

$$s'v' \equiv s'z' \equiv s'y' \equiv 0 \pmod{p}.$$

At least one of the three quantities v', z' or y' is prime to p, since otherwise s' may be taken $= 1$.

Let

$$R_1'^{s''} = Q_1'^{s'} P_1'^{sp^{m-4}},$$

or in terms of S', R', Q' and P'

$$[s''v'', s''z'' + c'\tbinom{s''}{2}v''y'', s''y'' + g'\tbinom{s''}{2}v''z'', Ep^{m-4}]$$
$$= [s'v', s'z' + c'\tbinom{s'}{2}v'y', s'y' + g'\tbinom{s'}{2}v'z', E_1p^{m-4}],$$

and

$$s''v'' \equiv s'v' \pmod{p},$$

$$s''z'' + c'\tbinom{s''}{2}v''y'' \equiv s'z' + c'\tbinom{s'}{2}v'y' \pmod{p},$$

$$s''y'' + g'\tbinom{s''}{2}v''z'' \equiv s'y' + g'\tbinom{s'}{2}v'z' \pmod{p}.$$

Since $c'g' \equiv 0 \pmod{p}$, suppose $g' \equiv 0 \pmod{p}$. Elimination of s' between the last two give by means of the congruence $Z_3' \equiv Z_3 \pmod{p}$,

$$s''\{2(y'z'' - y''z') + c'y'y''(v' - v'')\} \equiv 0 \pmod{p},$$

between the first two

$$s''\{2(v'z'' - v''z') + c'v'v''(y' - y'')\} \equiv 0 \pmod{p},$$

and between the first and last

$$s''(y'v'' - y''v') \equiv 0 \pmod{p}.$$

At least one of the three above coefficients of s'' is prime to p, since otherwise s'' may be taken $= 1$.

Let

$$S_1'^{s'''} = R_1'^{s''} Q_1'^{s'} P_1'^{sp^{m-4}}$$

or, in terms of S', R', Q', and P'

$$[s'''v''',\ s'''z''' + c'\tbinom{s'''}{2}v'''y''',\ s'''y''' + g'\tbinom{s'''}{2}v'''z''',\ E_2 p^{m-4}]$$

$$= [s''v'' + s'v',\ s''z'' + s'z' + c'\{\tbinom{s''}{2}v''y'' + \tbinom{s'}{2}v'y' + s's''y''v'\},$$

$$s''y'' + s'y' + g'\{\tbinom{s''}{2}v''z'' + \tbinom{s'}{2}v'z' + s's''v'z''\},\ E_3 p^{m-4}]$$

and

$$s'''v''' \equiv s''v'' + s'v' \pmod{p},$$

$$s'''z''' + c'\tbinom{s'''}{2}v'''y''' \equiv s''z'' + s'z' + c'\{\tbinom{s''}{2}v''y'' + \tbinom{s'}{2}v'y' + s's''y''v'\} \pmod{p},$$

$$s'''y''' + g'\tbinom{s'''}{2}v'''z''' \equiv s''y'' + s'y' + g'\{\tbinom{s''}{2}v'z'' + \tbinom{s'}{2}v'z' + s's''z''v'\} \pmod{p}.$$

If $g' \equiv 0$ and $c' \not\equiv 0 \pmod{p}$ the congruence $Z_3' \equiv Z_3 \pmod{p}$ gives

$$(y'v'' - y''v') \equiv 0 \pmod{p}.$$

Elimination in this case of s'' between the first and last congruences gives

$$s'''(y''v''' - y'''v'') \equiv 0 \pmod{p}.$$

Elimination of s'' between the first and second, and between the second and third, followed by elimination of s' between the two results, gives

$$s'''\left(z''^2 - c'y''z''v' + \frac{c'^2}{4}y''v'\right)(y'v''' - y'''v') \equiv 0 \pmod{p}.$$

Either $(y''v''' - y'''v'')$, or $(y'v''' - y'''v')$ is prime to p, since otherwise s''' may be taken $= 1$.

A similar set of conditions holds for $c' \equiv 0$ and $g' \not\equiv 0 \pmod{p}$.

When $c' \equiv g' \equiv 0 \pmod{p}$ elimination of s' and s'' between the three congruences gives

$$s'''\Delta \equiv s''' \begin{vmatrix} v' & v'' & v''' \\ y' & y'' & y''' \\ z' & z'' & z''' \end{vmatrix} \equiv 0 \pmod{p}$$

and Δ is prime to p, since otherwise s''' may be taken $= 1$.

7. *Reduction to types.* In the discussion of congruences (32), the group G' is taken from the simplest case and we associate with it all simply isomorphic groups G.

I.

A.

	a_2	β_2	c_2	g_2	γ_2	δ_2
1	1	1	1	1	1	1
2	0	1	1	1	1	1
3	0	0	1	1	1	1
4	0	0	1	1	1	0
5	0	0	1	0	1	1
6	0	0	1	0	1	0
7	0	1	0	1	1	1
8	0	1	0	1	0	1
9	0	1	1	0	1	1
10	0	1	1	0	1	0
11	1	0	1	1	1	1
12	1	0	1	0	1	1
13	1	0	1	1	0	1
14	1	0	1	1	1	0
15	1	0	1	0	0	1
16	1	0	1	0	1	0
17	1	0	1	1	0	0
18	1	0	1	0	0	0
19	1	1	0	1	1	1
20	1	1	0	1	0	1
21	1	1	0	1	1	0
22	1	1	0	1	0	0
23	1	1	1	0	1	1
24	1	1	1	1	0	1
25	1	1	1	1	1	0
26	1	1	1	0	0	1
27	1	1	1	0	1	0
28	1	1	1	1	0	0
29	1	1	1	0	0	0

B.

	k_2	α_2	ϵ_2	e_2	j_2
1	1	1	1	1	1
2	0	1	1	1	1
3	1	0	1	1	1
4	1	1	0	1	1
5	1	1	1	0	1
6	1	1	1	1	0
7	0	0	1	1	1
8	0	1	0	1	1
9	0	1	1	0	1
10	0	1	1	1	0
11	1	0	0	1	1
12	1	0	1	0	1
13	1	0	1	1	0
14	1	1	0	0	1
15	1	1	0	1	0
16	1	1	1	0	0
17	0	0	0	1	1
18	0	0	1	0	1
19	0	0	1	1	0
20	0	1	0	0	1
21	0	1	0	1	0
22	0	1	1	0	0
23	1	0	0	0	1
24	1	0	0	1	0
25	1	0	1	0	0
26	1	1	0	0	0
27	0	0	0	0	1
28	0	0	0	1	0
29	0	0	1	0	0
30	0	1	0	0	0
31	1	0	0	0	0
32	0	0	0	0	0

II.

A.

B.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	$\times$	$\times$	$\times$		19_6		19_6		19_6		$\times$	19_1	$\times$	11_1	19_1	19_1	13_1	19_1	$\times$	19_1	19_1	19_1	19_1	11_1	11_1	19_1	19_1	11_1	19_1
2	$\times$	2_1	3_1			19_6	19_6			19_6	25_2		$\times$	25_2			13_2		$\times$	19_2	$\times$	21_2		$\times$	$\times$			25_2	
3	1_2	2_1	3_1		19_6			19_6	19_6		11_1	19_2	13_1	24_2	21_2	19_2	13_1	21_2					19_2	25_2	24_2	21_2	19_2	25_2	21_2
4	1_2	$\times$	$\times$		19_6		19_6		19_6		24_2	19_2	13_1	24_2	19_1	19_2	13_1	19_1	19_2	19_2	19_1	19_1	19_2	11_1	11_1	19_1	19_2	11_1	19_1
5	2_1	2_1		*		19_6	19_6		19_6										19_1	19_2	19_1	19_1	19_6	11_6	3_1	21_6	19_6	3_1	21_6
6	2_1	2_1	3_1		19_6		19_6		19_6		$\times$	19_2	$\times$	11_6	21_2	19_2	13_6	21_2	$\times$	19_6	$\times$	21_6	19_1	3_1	11_6	19_1	19_2	3_1	19_1
7	1_2	2_1	3_1			19_6		19_6		19_6	25_2		13_2	25_2			13_2							25_2	25_2			*	
8	1_2	2_4	3_4			19_6	19_6			19_6	25_2		13_2	25_2			13_2		19_2	19_2	21_2	21_2		24_2	25_2			25_2	
9	2_1	2_1		*	19_6	19_6	19_6			19_6		19_6			21_6	19_6		21_6	19_2	19_2	21_2	21_2		11_6	3_1			3_1	
10	2_4	2_4	3_4			19_6	19_6			19_6	25_{10}		$\times$	25_{10}			13_{10}		19_6	19_6	21_6	21_6		3_4	$\times$			3_4	
11	1_2	2_4	3_4		19_6			19_6	19_6		24_2	19_2	13_1	*	21_2	19_2	13_1	21_2					19_2	25_2	24_2	21_2	19_2	25_2	21_2
12	2_4	2_4		*		19_6		19_6	19_6														19_6	25_{10}	3_4	21_6	19_6	3_4	21_6
13	2_1	2_1	3_1		19_6			19_6	19_6		11_6	*	13_6	11_6	*	19_2	13_6	*					19_2	3_1	11_6	21_2	19_2	3_1	21_2
14	2_1	2_4		*		19_6	19_6		19_6										19_2	*	19_1	19_1	19_6	11_6	3_1	21_6	19_6	3_1	21_6
15	2_1	2_4	3_4		19_6		19_6		19_6		11_6	19_2	13_6	11_6	21_2	19_2	13_6	21_2	19_6	19_6	21_6	21_6	19_2	3_1	11_6	19_1	*	3_1	19_1
16	2_1	2_1		*		19_6	19_6		19_6										19_6	19_6	21_6	21_6	19_6	3_1	3_1	21_6	19_6	*	21_6
17	1_2	2_4	3_4			19_6		19_6		19_6	25_2		13_2	25_2			13_2							25_2	25_2			*	
18	2_4	2_4		*	19_6	19_6		19_6		19_6		19_6			21_6	19_6		21_6						25_{10}	3_4			3_4	
19	2_4	2_4	3_4			19_6		19_6		19_6	25_{10}		13_{10}	25_{10}			13_{10}							3_4	25_{10}			3_4	
20	2_1	2_4		*	19_6	19_6	19_6			19_6		19_6			21_6	19_6		21_6	19_2	19_2	21_2	21_2		11_6	3_1			3_1	
21	2_4	*	*			19_6	19_6			19_6	25_{10}		13_{10}	25_{10}			13_{10}		19_6	19_6	21_6	21_6		3_4	25_{10}			3_4	
22	2_4	2_4		*	19_6	19_6	19_6			19_6		19_6			21_6	19_6		21_6	19_6	19_6	21_6	21_6		3_4	3_4			*	
23	2_4	*		*		19_6		19_6	19_6														19_6	25_{10}	3_4	21_6	19_6	3_4	21_6
24	2_1	2_4	3_4		19_6			19_6	19_6		11_6	19_2	13_6	11_6	*	*	13_6	*					19_2	3_1	11_6	21_2	19_2	3_1	21_2
25	2_4	2_4		*		19_6		19_6	19_6												21_6	21_6	19_6	3_4	3_4	21_6	19_6	*	21_6
26	2_1	2_4		*		19_6	19_6		19_6										19_6	19_6	21_6	21_6	19_6	3_1	3_1	21_6	19_6	*	21_6
27	2_4	*		*	19_6	19_6		19_6		19_6		19_6			21_6	19_6		21_6						25_{10}	3_4			3_4	
28	2_4	*	*			19_6		19_6		19_6	25_{10}		13_{10}	25_{10}			13_{10}							3_4	25_{10}			3_4	
29	*	*		*	19_6	19_6		19_6		19_6		19_6			21_6	19_6		21_6						*	*			*	
30	2_4	*		*	19_6	19_6	19_6			19_6		19_6			21_6	19_6		21_6	19_6	19_6	21_6	21_6		3_4	3_4			*	
31	2_4	*		*		19_6		19_6	19_6														19_6	3_4	3_4	21_6	19_6	*	21_6
32	*	*		*	19_6	19_6		19_6		19_6		19_6			21_6	19_6		21_6						*	*			*	

For convenience the groups are divided into cases.

The double Table I gives all cases consistent with congruences (17), (21), (23) and (25). The results of the discussion are given in Table II. The cases in Table II left blank are inconsistent with congruences (22) and (24), and therefore have no groups corresponding to them.

Let $\kappa = \kappa_1 p^{k_2}$ where $dv[\kappa_1, p] = 1$ $(\kappa = a, \beta, c, g, \gamma, d, k, \alpha, \epsilon, e, j)$.

In explanation of Table II the groups in cases marked $\boxed{r_s}$ are simply isomorphic with groups in $A_r B_s$.

The group G' is taken from the cases marked $\boxed{\times}$. The types are also selected from these cases.

The cases marked $\boxed{*}$ divide into two or more parts. Let

$$
\begin{aligned}
a\epsilon - \alpha e + jk &= I_1, & \alpha\epsilon - jk &= I_2,\\
a\delta(a - e) + 2I_1 &= I_3, & \alpha g - \beta j &= I_4,\\
\alpha\delta - \beta\epsilon &= I_5, & \epsilon g - \delta j &= I_6,\\
c\epsilon - e\gamma &= I_7, & \alpha e - jk &= I_8,\\
\delta e + \gamma j &= I_9, & \alpha\gamma + \delta k &= I_{10}.
\end{aligned}
$$

The parts into which these groups divide, and the cases with which they are simply isomorphic, are given in Table III.

III.

$A_{1,2}B^*$	$dv\,[I_1, p] = p$	2_1	$dv\,[I_1, p] = 1$	2_4
A_3B^*	$dv\,[I_2, p] = p$	3_1	$dv\,[I_2, p] = 1$	3_4
A_4B^*	$dv\,[I_3, p] = p$	3_1	$dv\,[I_3, p] = 1$	3_4
$A_{12}B_{13}$	$dv\,[I_4, p] = p$	19_1	$dv\,[I_4, p] = 1$	19_2
$A_{14}B_{11}$	$dv\,[I_5, p] = p$	11_1	$dv\,[I_5, p] = 1$	24_2
$A_{15,18}B^*$	$dv\,[I_4, p] = p$	19_1	$dv\,[I_4, p] = 1$	21_2
$A_{18}B_{24}$	$dv\,[I_6, I_5, p] = p$	19_1	$dv\,[I_6, I_5, p] = 1$	19_2
$A_{20}B_{14}$	$dv\,[I_7, p] = p$	19_1	$dv\,[I_7, p] = 1$	19_2
$A_{24,25}B^*$	$dv\,[I_8, p] = p$	3_1	$dv\,[I_8, p] = 1$	3_4
$A_{27}B_{15}$	$dv\,[I_6, p] = p$	19_1	$dv\,[I_6, p] = 1$	19_2
$A_{29}B_{7,17}$	$dv\,[I_{10}, p] = p$	24_2	$dv\,[I_{10}, p] = 1$	25_2
$A_{29}B_{16,28}$	$dv\,[I_9, p] = p$	11_6	$dv\,[I_9, p] = 1$	3_1
$A_{29}B_{22,25,30,31}$	$dv\,[I_9, p] = p$	25_{10}	$dv\,[I_9, p] = 1$	3_4
$A_{29}B_{29,32}$	$dv\,[I_8, I_9, p] = p$	11_6	$[I_8, p] = p,\ [I_9, p] = 1$	3_1
$A_{29}B_{29,32}$	$[I_8, p] = 1,\ [I_9, p] = p$	25_{10}	$[I_8, p] = 1,\ [I_9, p] = 1$	3_4

8. *Types.* The types for this class are given by equations (30) where the constants have the values given in Table IV.

IV.

	a	β	c	g	γ	δ	k	u	ε	e	j
1_1	0	0	0	0	0	0	0	0	0	0	0
2_1	1	0	0	0	0	0	0	0	0	0	0
3_1	κ	1	0	0	0	0	0	0	0	0	0
11_1	0	1	0	0	0	0	0	0	0	0	0
* 13_1	0	1	0	0	1	0	0	0	0	0	0
19_1	0	0	1	0	0	0	0	0	0	0	0
1_2	0	0	0	0	0	0	1	0	0	0	0
* 13_2	0	1	0	0	1	0	1	0	0	0	0
19_2	0	0	1	0	0	0	1	0	0	0	0
* 21_2	0	0	1	0	0	1	1	0	0	0	0
24_2	0	0	0	0	1	0	1	0	0	0	0
25_2	0	0	0	0	0	1	1	0	0	0	0
2_4	1	0	0	0	0	0	0	0	1	0	0
3_4	κ	1	0	0	0	0	0	0	1	0	0
11_6	0	1	0	0	0	0	0	0	0	0	1
* 13_6	0	1	0	0	1	0	0	0	0	0	1
19_6	0	0	1	0	0	0	0	0	0	0	1
* 21_6	0	0	1	0	0	1	0	0	0	0	1
* 13_{10}	0	1	0	0	κ	0	1	0	0	0	1
25_{10}	0	0	0	0	0	1	1	0	0	0	1

$\kappa = 1$, and a non-residue (mod p).

* For $p = 3$ these groups are isomorphic with groups in Class II.

A detailed analysis of congruences (32) for several cases is given below as a general illustration of the methods used.

$$A_3 B_1.$$

The special forms of the congruences for this case are

(II) $$\beta' x z' \equiv 0 \pmod{p},$$

(III) $$\alpha'(y z' - y' z) \equiv k x \pmod{p},$$

(IV), (V), (VI) $$\beta v' \equiv 0, \qquad \beta z' \equiv 0, \qquad \beta y' \equiv \beta' x z'' \pmod{p},$$

(VII) $$\alpha'(y z'' - y'' z) + \alpha' \beta' x \tbinom{z''}{2} \equiv \alpha x + \beta x' + \alpha' \beta y' z \pmod{p},$$

(X) $$\alpha'(y' z'' - y'' z') \equiv a x \pmod{p},$$

(XI) $$\gamma v'' + \delta v' \equiv 0 \pmod{p},$$

(XII) $$\gamma z'' + \delta z' \equiv 0 \pmod{p},$$

(XIII) $$\gamma y'' + \delta y' \equiv \beta' x z'' \pmod{p},$$

(XIV) $$\alpha'(y z''' - y''' z) + \alpha' \beta' x \tbinom{z'''}{2} \equiv e x + \gamma x'' + \delta x + \alpha' \delta y' z + \alpha' \gamma y'' z + \alpha' \tbinom{\gamma}{2} y'' z'' \pmod{p}.$$

(XV), (XVI), (XVII) $$c v'' \equiv 0, \qquad c z'' \equiv 0, \qquad c y'' \equiv 0 \pmod{p},$$

(XVIII) $$\alpha'(y' z''' - y''' z') \equiv e x \pmod{p},$$

(XIX), (XX), (XXI) $$g v' \equiv 0, \qquad g z' \equiv 0, \qquad g y' \equiv 0 \pmod{p},$$

(XXII) $$\alpha'(y'' z''' - y''' z'') \equiv j x \pmod{p},$$

From (II) $z' \equiv 0 \pmod{p}$.

The conditions of isomorphism give

$$\Delta \equiv \begin{vmatrix} v' & v'' & v''' \\ y' & y'' & y''' \\ z' & z'' & z''' \end{vmatrix} \not\equiv 0 \pmod{p}.$$

Multiply (IV), (V), (VI) by γ and reduce by (XII), $\beta\gamma v' \equiv 0$, $\beta\gamma z' \equiv 0$, $\beta\gamma y' \equiv 0 \pmod{p}$. Since $\Delta \not\equiv 0 \pmod{p}$, one at least of the quantities, v', z' or y' is $\not\equiv 0 \pmod{p}$ and $\beta\gamma \equiv 0 \pmod{p}$.

From (XV), (XVI) and (XVII) $c \equiv 0 \pmod p$, and from (XIX), (XX) and (XXI) $g \equiv 0 \pmod p$.

From (IV), (V), (VI) and (X) if $a \equiv 0$, then $\beta \equiv 0$ and if $a \not\equiv 0$, then $\beta \not\equiv 0 \pmod p$.

At least one of the three quantitis β, γ or δ is $\not\equiv 0 \pmod p$ and one, at least, of a, e or j is $\not\equiv 0 \pmod p$.

A_3: Since $z''' \equiv 0 \pmod p$, (XVIII) gives $e \equiv 0$. Elimination between (III), (X), (XIV) and (XXII) gives $a\epsilon - kj \equiv 0 \pmod p$. Elimination between (VI) and (X) gives $a'\beta' z''^2 \equiv a\beta \pmod p$ and $a\beta$ is a quadratic residue or non-residue according as $a'\beta'$ is or is not, and there are two types for this case.

A_4: Since y' and z''' are $\not\equiv 0 \pmod p$, $e \not\equiv 0 \pmod p$. Elimination between (VI), (X), (XIII) and (XVIII) gives $a\delta - \beta e \equiv 0 \pmod p$.

This is a special form of (24).

Elimination between (III), (VII), (X), (XIII), (XIV), (XVIII) and (XXII) gives

$$2jk + a\delta(a - e) + 2(a\epsilon - \alpha e) \equiv 0 \pmod p.$$

A_{24}: Since from (XI), (XII) and (XIII) y'' and $z''' \not\equiv 0 \pmod p$, and $z'' \equiv v'' \equiv 0 \pmod p$, (XXII) gives $j \not\equiv 0 \pmod p$.

Elimination between (III), (X), (XVIII) and (XXII) gives

$$\alpha e - jk \equiv 0 \pmod p.$$

A_{25}: (XI), (XII) and (XIII) give $v' \equiv z' \equiv 0$ and $y', z''' \not\equiv 0 \pmod p$ and this with (XVIII) gives $e \not\equiv 0$.

Elimination between (III), (VII), (XVIII) and (XXII) gives

$$\alpha e - jk \equiv 0 \pmod p.$$

A_{28}: Since $a \equiv 0$ then e or $j \not\equiv 0 \pmod p$.

Elimination between (III), (VII), (XVIII) and (XXII) gives

$$\alpha e - jk \equiv 0 \pmod p.$$

Multiply (XIII) by $a'z'''$ and reduce

$$\delta e + \gamma j \equiv a'\beta' z'''^2 \not\equiv 0 \pmod p.$$

$A_{11} B_1$.

The special forms of the congruences for this case are

(II) $$\beta' x z' \equiv 0 \pmod{p},$$

(III) $$k x \equiv 0 \pmod{p},$$

(IV), (V), (VI) $$\beta v' \equiv \beta z' \equiv 0, \qquad \beta y' \equiv \beta' x z'',$$

(VII) $$\alpha x + \beta x' \equiv 0 \pmod{p},$$

(X) $$a x \equiv 0 \pmod{p},$$

(XI) $$\gamma v'' + \delta v \equiv 0 \pmod{p},$$

(XII) $$\gamma z'' + \delta z \equiv 0 \pmod{p},$$

(XIII) $$\gamma y'' + \delta y \equiv \beta' x z''' \pmod{p},$$

(XIV) $$\epsilon x + \gamma x'' + \delta x' \equiv 0 \pmod{p},$$

(XV), (XVI), (XVII) $$c v'' \equiv c z'' \equiv c y'' \equiv 0 \pmod{p},$$

(XVIII) $$e x \equiv 0 \pmod{p}.$$

(XIX), (XX), (XXI) $$g v' \equiv g z' \equiv g y' \equiv 0 \pmod{p},$$

(XXII) $$j x \equiv 0 \pmod{p}.$$

(II) gives $z' = 0$, (III) gives $k \equiv 0$, (X) gives $a \equiv 0$, (XV), (XVI), (XVII) give $c \equiv 0$ ($\Delta \not\equiv 0$), (XVIII) gives $e \equiv 0$, (XIX), (XX), (XXI) give $g \equiv 0$, (XXII) gives $j \equiv 0$. One of the two quantities z'' or $z''' \not\equiv 0 \pmod{p}$, and by (VI) and (XIII) one of the three quantities β, γ or δ is $\not\equiv 0$.

A_{11}: (XIV) gives $\epsilon \equiv 0 \pmod{p}$. Multiplying (IV), (V), (VI) by γ gives, by (XII), $\beta\gamma v' \equiv \beta\gamma z' \equiv \beta\gamma y' \equiv 0 \pmod{p}$, and $\beta\gamma \equiv 0 \pmod{p}$.

A_{14}: Elimination between (VII) and (XIV) gives $\alpha\delta - \beta\epsilon \equiv 0 \pmod{p}$.

A_{24}: (VII) gives $\alpha \equiv 0 \pmod{p}$, (XIV) $\epsilon \equiv 0$ or $\not\equiv 0 \pmod{p}$.

A_{25}: (VII) gives $\alpha \equiv 0 \pmod{p}$, (XIV) $\epsilon \equiv$ or $\not\equiv 0 \pmod{p}$.

A_{28}: (VII) gives $\alpha \equiv 0 \pmod{p}$, (XIV) $\epsilon \equiv$ or $\not\equiv 0 \pmod{p}$.

$A_{19} B_1$.

The special forms of the congruences for this case are

(I) $$c' (y v' - y' v) \equiv 0 \pmod{p},$$

(III) $kx \equiv 0 \pmod p$,

(IV), (V), (VI) $\beta v \equiv 0$, $\beta z \equiv c'(yv'' - y''v)$, $\beta y' \equiv 0 \pmod p$,

(VII) $ax + \beta x' \equiv 0 \pmod p$,

(VIII) $c'(y'v'' - y''v') \equiv 0 \pmod p$,

(X) $ax \equiv 0 \pmod p$,

(XI) $\gamma v'' + \delta v' \equiv 0 \pmod p$,

(XII) $\gamma z'' + \delta z' + c'\gamma\delta y''v + c'\binom{\delta}{2}v'y' + c'\binom{\gamma}{2}v''y'' \equiv c'(yv''' - y'''v) \pmod p$,

(XIII) $\gamma y'' + \delta y' \equiv 0 \pmod p$,

(XIV) $\epsilon x + \gamma x'' + \delta x' \equiv 0 \pmod p$,

(XV), (XVI), (XVII) $cv'' \equiv 0$, $cz'' \equiv c'(y'v''' - y'''v')$, $cy'' \equiv 0 \pmod p$,

(XVIII) $ex + cx'' \equiv 0 \pmod p$,

(XIX), (XX), (XXI) $gv' \equiv 0$, $gz' \equiv c'(y''v''' - y'''v'')$, $gy' \equiv 0 \pmod p$,

(XXII) $jx + gx' \equiv 0 \pmod p$.

(III) gives $k \equiv 0$, (X) gives $a \equiv 0$.

Since $dv\ [(y'v''' - y'''v'), (y''v''' - y'''v''), p] = 1$ then $dv\ [c, g, p] = 1$.

If $c \not\equiv 0$, $v'' \equiv y'' \equiv 0 \pmod p$ and therefore $g \equiv 0 \pmod p$ and if $g \not\equiv 0$, then $c \equiv 0 \pmod p$.

A_{12}: (XVIII) gives $e \equiv 0 \pmod p$. Elimination between (VII) and (XXII) gives $ag - \beta j \equiv 0 \pmod p$, (XIV) gives $\epsilon \equiv 0 \pmod p$.

A_{15}: (XVIII) gives $e \equiv 0 \pmod p$. Elimination between (VII) and (XXII) gives $ag - \beta j \equiv 0 \pmod p$, (XIV) gives $\epsilon \equiv 0$ or $\not\equiv 0 \pmod p$.

A_{16}: (XVIII) gives $e \equiv 0$. Elimination between (XIV) and (XXII) gives $\epsilon g - \delta j \equiv 0 \pmod p$, between (VII) and (XIV) gives $a\delta - \beta\epsilon \equiv 0$.

A_{18}: (XVIII) gives $e \equiv 0$. Elimination between (VII) and (XXII) gives $ag - \beta j \equiv 0 \pmod p$, (XIV) gives $\epsilon \equiv 0$ or $\not\equiv 0 \pmod p$.

A_{19}: (VII) gives $a \equiv 0 \pmod p$, (XIV) gives $\epsilon \equiv 0$, (XXII) gives $j \equiv 0 \pmod p$, (XVIII) gives $e \equiv 0$ or $\not\equiv 0 \pmod p$.

A_{20}: (VII) gives $a \equiv 0$, (XXII) gives $j \equiv 0$. Elimination between (XIV) and (XVIII) gives $\epsilon c - e\gamma \equiv 0 \pmod p$.

A_{21}: (VII) gives $a \equiv 0$, (XIV) gives $\epsilon \equiv 0$ or $\not\equiv 0 \pmod p$, (XVIII) gives $e \equiv 0$, or $\not\equiv 0$, and (XXII) gives $j \equiv 0 \pmod p$.

A_{22}: (VII) gives $\alpha \equiv 0$, (XIV) gives $\epsilon \equiv 0$ or $\not\equiv 0$, (XVIII) gives $e \equiv 0$ or $\not\equiv 0$, (XXII) gives $j \equiv 0 \pmod{p}$.

A_{23}: (VII) gives $\alpha \equiv 0$, (XIV) gives $\epsilon \equiv 0$, (XVIII) gives $e \equiv 0$, (XXII) gives $j \equiv 0$ or $\not\equiv 0 \pmod{p}$.

A_{26}: (VII) $\alpha \equiv 0$, (XIV) $\epsilon \equiv 0$ or $\not\equiv 0$, (XVIII) $e \equiv 0$, (XXII) $j \equiv 0$ or $\not\equiv 0 \pmod{p}$.

A_{27}: (VII) $\alpha \equiv 0$, (XIV) $\epsilon \equiv 0$ or $\not\equiv 0$, (XVIII) $e \equiv 0$, (XXII) $j \equiv 0$ or $\not\equiv 0 \pmod{p}$. Elimination between (XIV) and (XXII) gives $\epsilon g - \delta j \equiv 0 \pmod{p}$.

A_{29}: (VII) $\alpha \equiv 0$, (XIV) $\epsilon \equiv 0$ or $\not\equiv 0$, (XVIII) $e \equiv 0$, (XXII) $j \equiv 0$ or $\not\equiv 0 \pmod{p}$.